Assurances

Assurances

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SOUS L'AILE DU FEDERAL

Divers collaborateurs du Groupe-conseil AON

Volume 69, Number 1, 2001

URI: https://id.erudit.org/iderudit/1105361ar
DOI: https://doi.org/10.7202/1105361ar

See table of contents

Publisher(s)

HEC Montréal

ISSN

0004-6027 (print)
2817-3465 (digital)

Explore this journal

Cite this document

collaborateurs du Groupe-conseil AON, D. (2001). LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SOUS L'AILE DU FEDERAL. *Assurances*, *69*(1), 143–150. https://doi.org/10.7202/1105361ar

Assurances, volume 69, numéro 1, avril 2001, 143-150

CHRONIQUE ACTUARIELLE

par divers collaborateurs du Groupe-conseil AON

■ LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SOUS L'AILE DU FÉDÉRAL

En avril 2000, le Canada s'est doté d'une loi ayant pour but la protection des renseignements personnels dans le secteur privé. L'entrée en vigueur de la *Loi sur la protection des renseignements personnels et les documents électroniques* (Loi) a pris son envol le 1er janvier 2001. La Loi comporte cinq volets. Nous nous attarderons ici au premier volet qui porte sur la protection des renseignements personnels.

Entrée en vigueur et mise en application

La Loi entrera progressivement en vigueur selon le type d'institution ou de renseignement visé. La première étape a pris effet le 1er janvier dernier. Elle vise les organisations provinciales qui, pour contrepartie, communiquent des renseignements à l'extérieur de la province. Elle touche également les entreprises et les organisations fédérales comme les banques, les sociétés de télécommunications, les compagnies aériennes, les entreprises ferroviaires et de transport interprovincial ainsi que les dossiers sur les employés de ces organisations.

Un moratoire d'un an est consenti aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels sur la santé. Pour ces organisations, la Loi s'appliquera seulement à partir du 1er janvier 2002.

Les provinces, quant à elles, ont jusqu'au 1er janvier 2004 pour se doter d'une loi similaire dans le cadre d'activités commerciales intraprovinciales, à défaut, la loi fédérale s'appliquera aux organisations de compétence provinciale à partir de cette

date. Il existe une seule exception, le Québec, qui s'est muni de deux lois portant sur la protection et l'accès à l'information et visant les entreprises publiques, parapubliques et privées. D'ailleurs, dans un communiqué du 1er octobre 1998, le gouvernement fédéral déclarait que les organisations provinciales basées au Québec seraient exemptées de l'application de sa Loi en ce qui concerne les renseignements recueillis, utilisés ou communiqués à l'intérieur de la province.

VOTRE ENTREPRISE EST-ELLE VISÉE?

Votre organisation est-elle une entreprise fédérale qui recueille, utilise ou communique des renseignements personnels dans le cadre d'une activité commerciale?

Si vous répondez « oui », votre organisation est visée par la Loi depuis le 1er janvier 2001. La Loi s'applique aux renseignements personnels concernant vos employés aussi bien que vos clients.

Si vous répondez « non », communiquez-vous des renseignements personnels, pour contrepartie, à l'extérieur de la province?

Si vous répondez « oui », la communication est visée par la Loi depuis le 1er janvier 2001.

Soulignons que l'application de la Loi s'étend aux associations, aux sociétés de personnes, aux personnes et aux organisations syndicales.

Principes directeurs

La Loi vise principalement la collecte, l'utilisation et la communication des renseignements personnels. Un renseignement personnel est défini comme étant tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et l'adresse et le numéro de téléphone de son lieu de travail.

Les renseignements personnels peuvent prendre plusieurs formes, notamment :

- Âge, nom, numéro d'immatriculation, revenu, origine ethnique ou type sanguin;

- Opinions, évaluations, commentaires ou statut social;
- Dossiers d'employé, dossiers de crédit, dossiers relatifs à des prêts, dossiers médicaux, propositions (par exemple, dossiers d'acquisition de biens ou de services ou de charges d'emploi).

Cette nouvelle Loi s'articule autour de dix principes directeur :

- Responsabilité
- Détermination des fins de la collecte des renseignements
- Consentement
- Limitation de la collecte
- Limitation de l'utilisation, de la communication et de la conservation des renseignements
- Exactitude
- Mesures de sécurité
- Transparence
- Accès aux renseignements personnels
- Possibilité de porter plainte à l'égard du non-respect des principes

L'application de ces principes a pour effet de prohiber toute collecte, divulgation et utilisation de renseignements personnels effectuées à l'insu de l'intéressé ou sans son consentement, sauf dans certains cas spécifiquement prévus dans la Loi.

Le consentement et les fins visées

Pour que le consentement soit valable, les fins visées doivent être énoncées de façon à ce que l'intéressé puisse raisonnablement comprendre de quelle manière les renseignements seront recueillis, utilisés ou communiqués. L'avis doit se faire avant ou au moment même de la collecte.

L'organisation doit dorénavant se limiter à recueillir les renseignements qui sont nécessaires aux fins qu'elle détermine et doit procéder de façon honnête et licite.

Les personnes qui recueillent l'information doivent être en mesure d'expliquer les raisons et le but de la collecte.

Quant à savoir si le consentement doit être fourni par écrit, tout dépend de la sensibilité des renseignements, compte tenu de leur nature et des circonstances s'y rattachant. Il faut aussi prendre en considération les attentes raisonnables de l'intéressé à l'égard de la protection des renseignements personnels le concernant. Par exemple, il va de soi qu'une personne est en mesure de s'attendre à ce qu'un plus grand soin soit apporté à la gestion de l'information médicale ou financière la concernant qu'à l'utilisation de renseignements moins personnels telle la marque de son automobile. Il est donc plus indiqué d'exiger un consentement écrit dans le premier cas que dans le second.

Aucune forme particulière n'est requise pour le consentement. Il peut s'agir d'un formulaire distinct, d'une case à cocher ou d'un consentement verbal lors d'une transaction téléphonique, selon la sensibilité de l'information en question.

Mesures de sécurité

La Loi oblige les organisations à prendre diverses mesures de sécurité afin d'assurer la protection des renseignements personnels. Elles devront :

- désigner une personne responsable du respect des dix principes directeurs;
- élaborer une politique de protection des renseignements;
- définir des pratiques à l'égard de la mise en œuvre de la politique, notamment pour recevoir les plaintes et les demandes de renseignements et pour y donner suite;
- sensibiliser les employés sur l'importance de protéger le caractère confidentiel des renseignements personnels auxquels ils ont accès et les informer sur la politique et les pratiques à suivre, et ce, à toutes les étapes de la manipulation des renseignements; de la collecte jusqu'à la destruction;
- rédiger des documents explicatifs sur la politique et les pratiques; ceux-ci devront être mis à la disposition de toute personne qui en fait la demande (voir l'encadré ci-après);
- détruire, effacer ou dépersonnaliser les renseignements qui ne sont plus nécessaires aux fins précisées;
- prendre les mesures de sécurité appropriées selon le degré de sensibilité des renseignements à l'aide de moyens

matériels (verrouillage des classeurs, restriction de l'accès aux classeurs), de mesures administratives (accès sélectifs) et d'outils technologiques (mot de passe).

TRANSPARENCE

Toute organisation doit pouvoir fournir sur demande ou rendre facilement accessibles les renseignements suivants :

- le nom ou la fonction ainsi que l'adresse de la personne responsable de la politique et des pratiques en matière de protection de renseignements personnels;
- le nom ou la fonction ainsi que l'adresse de la personne à qui les plaintes et les demandes de renseignements doivent être acheminées;
- une description du genre de renseignements personnels que possède l'organisation et des explications générales sur l'usage auquel ils sont destinés;
- une copie de toute brochure ou de tout autre document d'information expliquant la politique, les normes ou les codes de l'organisation en matière de gestion des renseignements personnels;
- une définition de la nature des renseignements personnels communiqués à d'autres organisations (y compris les filiales).

La façon dont ces renseignements sont rendus accessibles dépend, entre autres, de la nature des activités de l'organisation.

Droits des personnes intéressées

Toute personne dont les renseignements personnels font l'objet d'une collecte, d'une communication ou d'une utilisation se voit conférer divers droits que l'organisation devra respecter :

- Le droit d'être informée, sur demande, de toute collecte, utilisation ou communication des renseignements qui la concerne incluant celui d'obtenir la liste des personnes à qui l'information a été communiquée;

- Le droit de refuser toute collecte, utilisation ou communication de renseignements personnels, à moins que l'obtention du consentement ne soit pas appropriée dans les circonstances;
- Le droit de contester l'exactitude et l'intégralité des renseignements;
- Le droit d'y faire apporter les corrections appropriées;
- Le droit d'exiger que l'organisation utilise des renseignements aussi exacts, complets et à jour que possible.

Demande d'accès

On doit donner suite à toute demande d'accès à des renseignements personnels de façon diligente et au plus tard 30 jours suivant sa réception.

Le défaut de répondre dans le délai prévu équivaut à un refus et peut entraîner le dépôt d'une plainte. Si l'organisation exige des frais, elle doit informer le demandeur du montant approximatif de ceux-ci.

Les renseignements doivent être fournis sous une forme compréhensible. Si, par exemple, l'organisation collige l'information sous forme de codes ou d'abréviations, elle doit fournir les explications nécessaires à la compréhension des renseignements.

Tout refus doit être motivé par écrit et faire mention des recours disponibles. L'information qui révélerait vraisemblablement un renseignement personnel sur un tiers peut amener un refus sauf si ce renseignement peut être retranché de cette information.

Plainte et recours

La Loi prévoit trois niveaux de plaintes et de recours.

1er niveau La plainte doit tout d'abord être gérée au sein même de l'organisation, conformément au processus de plaintes et d'enquêtes qu'elle doit avoir mis en place.

2e niveau Une plainte peut être déposée auprès du Commissaire à la protection de la vie privée nommé conformément à la Loi. Lorsqu'elle porte sur un refus, la plainte doit être déposée dans les six mois

suivant le refus ou à l'expiration du délai prévu pour répondre à une demande d'accès. Le Commissaire doit produire son rapport dans l'année de la plainte et le remettre au plaignant et à l'organisation. Il peut assigner des témoins, par écrit ou verbalement, et recourir à la médiation et à la conciliation. La Loi ne lui confère cependant qu'un pouvoir de recommandation.

3e niveau Si le plaignant n'est pas satisfait des conclusions du rapport, il peut demander, dans les 45 jours suivant la transmission du rapport, à la section de première instance de la Cour fédérale de statuer sur la plainte. Le Commissaire peut également demander à être entendu par la Cour. La Cour fédérale a le pouvoir d'ordonner à l'organisation de revoir ses pratiques afin de se conformer à la Loi. La Cour peut aussi lui ordonner de publier des avis sur les mesures prises ou envisagées pour corriger ses pratiques et accorder des dommages et intérêts au plaignant.

Plan d'action

Voilà de bien intéressants principes mais où doit-on commencer? Dans un premier temps, il est important que les organisations soient sensibilisées à la nécessité de protéger l'information personnelle et qu'elles prennent les mesures nécessaires afin de communiquer le message à leurs employés et à leurs clients.

Ensuite, il devient nécessaire de dresser l'inventaire des renseignements personnels que détient l'organisation et de porter une attention toute particulière au cheminement de cette information. Un processus de questionnement s'impose. Il variera d'une organisation à l'autre et soulèvera des interrogations telles :

- À quelles fins les renseignements sont-ils recueillis, communiqués ou utilisés?
- Est-il vraiment nécessaire de recueillir les renseignements demandés?
- La personne visée par ces renseignements a-t-elle été informée des fins poursuivies?
- S'agit-il de renseignements dont le niveau de sensibilité est élevé?

Une fois l'inventaire dressé et les constats émis, il faut élaborer une politique de protection des renseignements ainsi que les procédures qui s'y rattachent, et mettre en œuvre les autres mesures de sécurité requises par la Loi.

Le processus de mise en place des mesures de sécurité peut sembler lourd mais il s'inscrit dans le cadre d'une préoccupation non seulement nationale mais mondiale.

L'Organisation de coopération et de développement économique a élaboré des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel* auxquelles le Canada a adhéré en 1984. L'OCDE recommandait que les pays membres en tiennent compte dans leur législation interne, ce que le Canada a fait avec sa nouvelle Loi qui reprend le *Code type sur la protection des renseignements personnels* adopté par l'Association canadienne de normalisation.

Soulignons qu'en 1995, l'Union européenne a émis, à l'intention de ses pays membres, une directive qui est entrée en vigueur en 1998. Cette directive les enjoignait de ne pas transmettre de renseignements personnels en provenance d'Europe à un pays qui ne peut offrir de protection législative comparable et qui n'a pas mis en place d'organisme de réglementation responsable d'en faire respecter l'application. Il devient ainsi d'autant plus important de se doter de mesures de protection à l'égard des renseignements personnels afin de ne pas nuire aux relations économiques que les entreprises canadiennes entretiennent avec les pays de l'Union européenne.

Force nous est de constater que la protection des renseignements personnels est désormais plus qu'un enjeu, c'est une réalité qu'il faut transposer en mode de vie.