12. Loi sur la protection des renseignements personnels et Loi canadienne anti-pourriel

Survol

Au Canada, la protection de la vie privée est régie par un ensemble de lois dans le secteur public, le secteur privé et le secteur de la santé, ainsi que par la *Loi canadienne anti-pourriel* (la « LCAP »). Selon le secteur, ces lois proviennent du palier fédéral et/ou du palier provincial. Des considérations de common law peuvent également s'appliquer. Le présent chapitre porte principalement sur la loi fédérale canadienne encadrant le secteur privé (compte tenu de son application générale aux entreprises canadiennes) et sur la conformité à la LCAP.

Secteur privé

LPRPDE

La *Loi sur la protection des renseignements personnels et les documents électroniques* (la « LPRPDE ») est la loi fédérale canadienne applicable au secteur privé. Elle régit la collecte, l'utilisation et la communication de renseignements personnels.

Définition de « renseignement personnel »

Dans la LPRPDE, le « renseignement personnel » est défini de manière générale comme étant « tout renseignement concernant un individu identifiable ». De tels renseignements peuvent inclure notamment le nom, l'adresse, le numéro de téléphone, l'âge, le sexe, l'ethnicité, la religion, l'éducation, ainsi que les renseignements sur la santé et sur la situation financière d'une personne. Certains renseignements fournis par le gouvernement sont également considérés comme des renseignements personnels, notamment le numéro d'assurance sociale, le numéro d'assurance-maladie provincial, le numéro de permis de conduire et le numéro de passeport.

La définition des renseignements personnels de la LPRPDE ne s'applique pas aux coordonnées d'affaires recueillies, utilisées ou communiquées uniquement pour entrer en contact avec un individu dans le cadre de son emploi, de son entreprise ou de sa profession.

Application de la LPRPDE

D'une manière générale, la LPRPDE s'applique à toute organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales, y compris :

- les organisations sous réglementation provinciale dans les provinces qui n'ont pas de lois sur la protection des renseignements personnels essentiellement similaires à la LPRPDE (l'Alberta, la Colombie-Britannique et le Québec ont leurs propres lois sur la protection des renseignements personnels dans le secteur privé jugées essentiellement similaires à la LPRPDE [1]);
- les organisations qui transfèrent des renseignements personnels d'un pays ou d'une province à l'autre.

La LPRPDE s'applique également à l'égard des renseignements personnels concernant les employés lorsque ces renseignements sont recueillis, utilisés ou communiqués dans le cadre d'une entreprise fédérale (comme les banques, les lignes aériennes et les autres entreprises de transport interprovinciales ou internationales, les entreprises de télécommunication, les entreprises exerçant des activités de forage en mer; et les radiodiffuseurs et télédiffuseurs).

À l'inverse, la LPRPDE ne s'applique pas aux renseignements personnels qu'une organisation recueille, utilise ou communique au sujet de ses employés si cette organisation relève de la compétence provinciale (c.-à-d. n'est pas une entreprise fédérale). Les principes généraux de la LPRPDE sont les suivants :

- 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
- Exactitude
- Mesures de sécurité
- Transparence
- Accès aux renseignements personnels
- Possibilité de porter plainte en cas de non-respect des principes

1 De plus, l'Ontario, le Nouveau-Brunswick, la Nouvelle-Écosse et Terre-Neuve-et-Labrador ont également adopté des lois essentiellement similaires dans le secteur de la santé.

La LPRPDE et votre entreprise

Connaissance et consentement

Le consentement éclairé est le principe directeur qui sous-tend la LPRPDE. Toute personne devrait être informée des fins pour lesquelles ses renseignements personnels sont recueillis, utilisés ou communiqués et devrait avoir le droit de consentir à de telles activités ou de les refuser. Le consentement n'est valide que s'il est raisonnable de penser que la personne intéressée comprend « la nature, les fins et les conséquences » de la collecte, de l'utilisation ou de la communication des renseignements personnels à laquelle elle consent.

La règle du consentement comporte certaines exceptions. Ainsi, une organisation est dispensée d'obtenir un consentement avant de recueillir des renseignements personnels lorsque cette collecte est dans l'intérêt de la personne visée et que son consentement ne peut être obtenu en temps opportun; le consentement n'est pas non plus exigé lorsqu'il s'agit d'un « renseignement auquel le public a accès » (la portée de cette notion est strictement délimitée par voie réglementaire). Une personne peut donner son consentement de diverses façons, notamment de manière expresse, de manière implicite ou par le biais d'un mécanisme d'exclusion. La forme appropriée de consentement qu'une organisation doit obtenir dépendra de la sensibilité des renseignements personnels en cause et des attentes raisonnables de la personne (compte tenu des circonstances).

Transactions commerciales

Il n'est pas rare que les organisations soient tenues de recueillir, d'utiliser ou de communiquer des renseignements personnels, y compris des renseignements personnels d'employés, dans le cadre de l'exécution d'une vérification préalable et de la conclusion d'une transaction commerciale.

La LPRPDE permet que ces activités soient menées sans obtenir de consentement, si :

- les organisations ont conclu un accord aux termes duquel le destinataire s'est engagé a) à n'utiliser les renseignements qu'à des fins liées à la transaction; b) à protéger les renseignements; ou c) à détruire ou à remettre les renseignements si la transaction est annulée;
- les renseignements personnels sont nécessaires pour décider si la transaction aura lieu ou non et, le cas échéant, pour l'effectuer
- pour les transactions effectuées, les organisations ont conclu un accord aux termes duquel elles s'engagent a) à n'utiliser et à ne communiquer les renseignements qu'aux fins pour lesquelles ils ont été recueillis, utilisés ou communiqués avant la transaction; b) à protéger les renseignements; et (c) à donner effet à tout retrait de consentement;

- les renseignements doivent être nécessaires pour effectuer l'activité faisant l'objet de la transaction et l'une des parties doit, dans un délai raisonnable, aviser les personnes de la transaction et de la communication.

La dispense ci-dessus ne s'applique pas si l'objectif premier de la transaction est l'achat (ou toute autre acquisition), la vente, la disposition ou la location de renseignements personnels. La dispense codifie la pratique courante et est élaborée selon des dispositions similaires à la législation en matière de respect de la vie privée de la Colombie-Britannique et de l'Alberta.

Impartition du traitement de données aux États-Unis

Les sociétés canadiennes peuvent impartir certaines activités de traitement des données à une société mère américaine ou à une entreprise tierce dans ce domaine établie aux États-Unis ou dans un autre pays. Même si la LPRPDE n'interdit pas l'impartition des activités de traitement des données, l'organisation canadienne demeure responsable des renseignements personnels lors de leur transfert à une tierce partie au nom de l'organisation.

De plus, l'organisation canadienne doit satisfaire aux deux exigences imposées par le Commissariat à la protection de la vie privée du Canada (le « Commissariat »). Premièrement, comme dans tout cas de traitement par un tiers (que celui-ci se fasse au Canada ou à l'étranger), l'organisation doit protéger la confidentialité et la sécurité des renseignements personnels soit en mettant en œuvre les mesures de sécurité appropriées, contractuelles ou d'une autre nature, entre l'organisation et la société mère (ou l'entreprise tierce de traitement), soit en s'assurant que la société mère et sa filiale sont régies par la même politique en matière de protection de la vie privée et sont tenues de satisfaire aux mêmes exigences en la matière. Deuxièmement, la filiale canadienne doit faire savoir aux personnes concernées que leurs renseignements personnels vont être conservés, utilisés ou communiqués à l'extérieur du Canada et que ces renseignements pourraient être accessibles aux termes des lois en vigueur dans le pays visé.

En plus des exigences ci-dessus, le Commissariat exige que les organisations canadiennes fassent preuve de diligence raisonnable à l'égard des exigences juridiques du pays où est établie la tierce partie qui traite les renseignements, de même qu'à « la situation politique, économique et sociale étrangère » qui peut nuire à sa capacité à protéger les renseignements personnels avant tout transfert. Le Commissariat demande aussi à ce que les organisations effectuent un suivi, une surveillance et une application appropriés des mesures de protection contractuelles et autres mentionnées ci-dessus.

Des exigences supplémentaires peuvent s'appliquer à certains types de renseignements et aux termes des lois provinciales sur la protection des renseignements personnels[2].

2 Par exemple, en vertu de la loi sur la protection des renseignements personnels de l'Alberta (la Personal Information Protection Act), lorsqu'une organisation fait appel à un fournisseur de services situé à l'extérieur du Canada, elle doit divulguer les pays étrangers où la collecte, l'utilisation et la communication des renseignements personnels peuvent avoir lieu.

Avis d'atteinte aux mesures de sécurité et tenue de registre

En vertu de la LPRPDE, les organisations sont tenues d'aviser les personnes (à moins qu'une règle de droit ne l'interdise) d'une atteinte aux mesures de sécurité et de la déclarer au Commissariat s'il est raisonnable de croire que l'atteinte présente un « risque réel de préjudice grave à l'endroit d'un individu ».

En vertu de la LPRPDE, un « préjudice grave » vise notamment les préjudices suivants : l'humiliation, le dommage à la réputation ou aux relations et le vol d'identité. Les éléments servant à établir si une atteinte présente un « risque réel » sont le degré de sensibilité des renseignements, la probabilité que les renseignements soient mal utilisés et tout autre élément prévu par règlement.

L'avis aux personnes et la déclaration au Commissariat doivent être donnés selon les modalités prévues et « le plus tôt possible » après conclusion qu'il y a eu atteinte. Le Commissariat peut publier de l'information relative à ces avis s'il juge qu'il est dans l'intérêt du public de le faire.

En vertu du *Règlement sur les atteintes aux mesures de sécurité* aux termes de la LPRPDE, l'avis à une personne doit contenir certains renseignements, y compris la description a) des circonstances de l'atteinte; b) des renseignements personnels visés par l'atteinte; c) des mesures prises par l'organisation pour réduire le préjudice qui pourrait en découler; et d) des mesures que la personne peut prendre pour réduire ou atténuer ce préjudice. L'avis doit être apparent et il doit être donné directement à l'individu, sauf dans certaines circonstances où un avis indirect (p. ex., l'affichage sur un site Web) pourrait être permis.

La déclaration au Commissariat doit contenir certains renseignements, notamment le nombre de personnes touchées, les coordonnées d'une personne qui peut répondre aux questions du Commissariat et une description a) des circonstances de l'atteinte; b) des renseignements personnels visés par l'atteinte; c) des mesures prises par l'organisation pour réduire le préjudice qui pourrait en découler; et d) des mesures prises par l'organisation pour informer les personnes touchées. La déclaration peut être envoyée par « tout moyen de communication sécurisé » et peut être mise à jour avec de nouveaux renseignements à mesure que l'organisation en prend connaissance.

En vertu de l'article 10.2 de la LPRPDE, les organisations qui avisent une personne sont tenues de transmettre un avis à tout autre organisation (p. ex. les agences d'évaluation du crédit) ou agence gouvernementale si elles peuvent, en agissant ainsi, permettre de réduire les risques de préjudice ou atténuer le préjudice. Le consentement n'est pas requis pour de telles communications.

En plus d'établir les exigences d'avis et de déclaration énoncées ci-dessus, la LPRPDE exige que les organisations tiennent et conservent un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elles ont la gestion. En vertu de l'article 6 du *Règlement sur les atteintes aux mesures de sécurité*, ce registre doit être

conservé pendant 24 mois après la date à laquelle l'organisation conclut qu'il y a eu atteinte. Il doit également contenir les renseignements nécessaires pour permettre au Commissariat de vérifier la conformité aux exigences en matière de déclaration et d'avis énoncées ci-dessus.

De plus, les organisations sont tenues de remettre de tels registres au Commissariat lorsque ce dernier en fait la demande. Le Commissariat peut publier des renseignements obtenus de ces registres s'il juge qu'une telle publication est dans l'intérêt du public.

Il est important de noter qu'aucun seuil n'est associé à l'obligation de tenue de registre; un registre de toutes les atteintes aux mesures de sécurité doit être tenu, que celles-ci posent ou non un risque réel de préjudice grave. De plus, il n'y a aucun seuil qu'une organisation doit atteindre avant d'être tenue de fournir ses « dossiers d'atteintes » au Commissariat.

Législation provinciale

Les provinces du Québec, de l'Alberta et de la Colombie-Britannique ont adopté des lois sur la vie privée dont la teneur est similaire à celle de la LPRPDE. Ainsi, la législation provinciale peut s'appliquer à la collecte, à l'utilisation ou à la communication des renseignements personnels dans les provinces visées (la LPRPDE s'applique aussi aux transferts interprovinciaux et internationaux de renseignements personnels et aux organisations sous réglementation fédérale).

Secteur public

Les lois fédérales, provinciales et territoriales régissent la collecte, l'utilisation et la communication de renseignements personnels par les organismes publics. De plus, la *Charte canadienne des droits et libertés* (la « Charte ») protège certains droits en matière de vie privée (p. ex., l'article 8 de la Charte accorde une protection de la vie privée personnelle, territoriale et informationnelle sous forme de « protection contre les fouilles, les perquisitions ou les saisies abusives » effectuées par le gouvernement). Le *Code criminel* prévoit également certaines mesures de protection de la vie privée; il établit notamment l'infraction de voyeurisme.

Secteur de la santé

La plupart des provinces et des territoires ont leur propre loi sur la protection des renseignements personnels en matière de santé. Ces lois s'appliquent aux fournisseurs de soins de santé, ainsi qu'à leurs fournisseurs de services et à leurs représentants. En plus de ces lois, les organismes de réglementation des professions de santé imposent également des exigences en matière de confidentialité des patients.

Modernisation des lois canadiennes sur la protection de la vie privée

Les gouvernements fédéral et provinciaux modernisent actuellement les lois canadiennes sur la protection de la vie privée. Au palier fédéral, la modernisation de la LPRPDE est en cours depuis un certain temps, et devrait donner lieu à un nouveau projet de loi prochainement.

Le Québec a adopté le projet de loi no 64, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* en 2020. Le projet de loi no 64 apportera des changements importants aux lois québécoises sur la protection de la vie privée dans le secteur privé et le secteur public. La plupart de ces changements entreront en vigueur à la fin de 2023 – même s'il reste à voir si certains de ces changements seront tempérés en faveur de l'harmonisation des lois canadiennes sur la protection de la vie privée entreprise par le gouvernement fédéral et les autres gouvernements provinciaux afin de moderniser leur législation en la matière.

Loi canadienne anti-pourriel

L'envoi de messages électroniques commerciaux (« MEC ») à destination et en provenance du Canada et l'installation de programmes d'ordinateur sur des systèmes situés au Canada sont régis par une loi communément appelée la *Loi canadienne anti-pourriel* (« LCAP ») et par son règlement d'application.

MEC

Un message électronique commercial est défini de manière très large dans la LCAP comme étant « un message électronique dont il est raisonnable de conclure, vu son contenu, le contenu de tout site Web ou autre banque de données auquel il donne accès par hyperlien ou l'information qu'il donne sur la personne à contacter, qu'il a pour but, entre autres, d'encourager la participation à une activité commerciale et, notamment, tout message électronique qui, selon le cas : a) comporte une offre d'achat, de vente, de troc ou de louage d'un produit, bien, service, terrain ou droit ou intérêt foncier; b) offre une possibilité d'affaires, d'investissement ou de jeu; c) annonce ou fait la promotion d'une chose ou possibilité mentionnée aux alinéas a) ou b); d) fait la promotion d'une personne, y compris l'image de celle-ci auprès du public, comme étant une personne qui accomplit – ou qui a l'intention d'accomplir – un des actes mentionnés aux alinéas a) à c) ».

Les demandes de consentement à la transmission d'un MEC sont également considérées comme des MEC; par conséquent, avant d'envoyer une telle demande, l'organisation doit étudier attentivement les exigences de la LCAP.

À la différence d'autres lois anti-pourriel comme la *CAN-SPAM Act* aux États-Unis, la LCAP institue un régime à option d'adhésion. À de rares exceptions près, la LCAP interdit l'envoi de MEC sauf en cas de consentement exprès ou tacite. Le consentement exprès doit être obtenu sous la forme prescrite par la LCAP. Le consentement tacite n'est possible que pour certaines catégories énumérées, notamment les « relations d'affaires en cours » telles que définies dans la loi.

De plus, chaque MEC doit indiquer les coordonnées de l'expéditeur et proposer un mécanisme d'exclusion.

Programmes d'ordinateur

D'une manière générale, la LCAP interdit l'installation de certains programmes d'ordinateur invasifs dans l'ordinateur d'une autre personne sans le consentement exprès du propriétaire ou de l'utilisateur autorisé de l'ordinateur ou en vertu d'une ordonnance judiciaire.

Cette interdiction s'applique si l'ordinateur se trouve au Canada au moment des actes reprochés ou si leur auteur soit se trouve au Canada à ce moment-là, soit agit sur les instructions d'une personne qui s'y trouve au moment où elle les lui donne.

D'autres exigences en matière d'avis et de consentement et d'autres obligations s'appliquent à l'égard des programmes qui effectuent certaines fonctions énumérées dans la loi ayant pour effet de faire fonctionner l'ordinateur d'une façon contraire aux attentes raisonnables du propriétaire ou de l'utilisateur autorisé de celui-ci, par exemple la collecte de renseignements personnels sur l'ordinateur.

Conséquences des contraventions à la LCAP

Les contraventions à la LCAP peuvent donner lieu à de lourdes sanctions pécuniaires (pouvant atteindre 10 millions de dollars pour les organisations), à l'engagement de la responsabilité des administrateurs et des dirigeants, ainsi qu'à une responsabilité élargie des personnes ayant participé à la contravention.