# 12.

# Lois sur la protection de la vie privée

## 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 un régime qui s'y rapporte dans la Loi canadienne anti-pourriel (la « LCAP ») dont il est question dans le chapitre Technologies de ce guide). Selon le secteur, ces lois proviennent du palier fédéral et/ou du palier provincial. Des considérations de common law peuvent également s'appliquer. Ce chapitre porte principalement sur la loi fédérale canadienne encadrant le secteur privé compte tenu de son application générale aux entreprises canadiennes.

## 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 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

De 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 en ce qui concerne les renseignements personnels recueillis, utilisés et communiqués dans des 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);
- 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. qu'elle n'est pas une entreprise fédérale). Comme nous l'avons souligné, la LPRPDE ne s'applique pas à la collecte, à l'utilisation ou à la communication de renseignements personnels par des organisations sous réglementation provinciale en Colombie-Britannique, en Alberta ou au Québec. 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.

## La LPRPDE et votre entreprise

### Connaissance et consentement

Le consentement éclairé est le principe directeur qui sous-tend la LPRPDE. Avant ou au moment de la collecte, 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 des lois provinciales de la Colombie-Britannique et de l'Alberta sur la protection de la vie privée.

### 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 l'autre entité, soit en s'assurant que ces entités 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, l'entité canadienne qui communique les renseignements personnels 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 de la vie privée.

### Signalement d'une atteinte aux mesures de sécurité et tenue d'un registre

Sauf si autrement interdit par la loi, la LPRPDE exige que les organisations avisent les personnes et le Commissariat de toute atteinte aux mesures de sécurité s'il est raisonnable de croire qu'elle 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 pris en application 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 manifeste et donné à l'intéressé directement, 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

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

Au Québec, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* est entrée en vigueur dans son intégralité en septembre 2024. Communément appelée la « loi 25 », elle a apporté des changements importants aux lois québécoises sur la protection des renseignements personnels dans les secteurs privé et public, entre autres. La loi 25 impose notamment les obligations suivantes aux entreprises établies au Québec :

- désigner un responsable de la protection des renseignements personnels chargé de veiller au respect des lois sur la protection de la vie privée (ce rôle sera attribué à la personne ayant la plus haute autorité dans l'entreprise si elle ne délègue pas cette fonction par écrit à quelqu'un d'autre);
- aviser la Commission d'accès à l'information et les personnes concernées si un incident de confidentialité « présente un risque qu'un préjudice sérieux soit causé »;

- réaliser des évaluations des facteurs relatifs à la vie privée dans diverses situations, notamment avant de traiter certains renseignements personnels dans le cadre de projets technologiques ou avant de communiquer des renseignements personnels à l'extérieur du Québec;
- permettre aux personnes concernées d'exercer de nouveaux droits, notamment le droit à la portabilité des données et le droit à la réindexation;
- payer des amendes d'un montant maximal de 25 000 000 $ CA ou d'un montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice précédent (le montant le plus élevé étant retenu), en cas de non-respect.

Les entreprises ayant des activités au Québec doivent tenir compte de ces dispositions.

### 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 et de publication d'images intimes.

### 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 du domaine de la santé imposent également des exigences en matière de confidentialité des patients.

### Modernisation des lois canadiennes sur la protection de la vie privée

Avec la généralisation et le développement de technologies soulevant des enjeux de protection de la vie privée, comme l'infonuagique et l'intelligence artificielle, la protection de la vie privée est devenue une préoccupation publique ces dernières années et fait désormais l'objet d'un suivi minutieux. Ainsi, les gouvernements fédéral et provinciaux travaillent actuellement à moderniser les lois canadiennes sur la protection de la vie privée, principalement dans le but de renforcer la sécurité entourant les renseignements personnels.

En effet, le 16 juin 2022, le gouvernement canadien a déposé le projet de loi C-27, la *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, qui remplacerait le cadre juridique de protection de la vie privée énoncé dans la LPRPDE par la *Loi sur la protection de la vie privée des consommateurs*.

Le projet de loi C-27 conserve les principes bien établis de la LPRPDE, fondés sur le consentement, selon lesquels les entreprises sont tenues d'obtenir le consentement de la personne concernée pour la collecte, l'utilisation et la communication de ses renseignements personnels. Toutefois, il offre aussi une certaine souplesse aux entreprises : a) en introduisant deux nouvelles exemptions au consentement pour « intérêt légitime » et « activités d'affaires », qui pourraient être invoquées par les entreprises dans la mesure où le traitement des renseignements personnels n'a pas pour but d'influencer le comportement ou les décisions d'une personne; et b) en autorisant le transfert des renseignements personnels à des fournisseurs de services sans le consentement des personnes concernées si les renseignements sont utilisés aux fins pour lesquelles ils ont été transférés et si des mécanismes de protection adéquats sont en place.

Le projet de loi C-27 répond aussi à la nécessité pour les lois canadiennes sur la protection de la vie privée d'évoluer au même rythme que les nouvelles technologies. En effet, il comprend de nouvelles définitions et protections connexes pour les renseignements dépersonnalisés et anonymisés en plus de proposer la *Loi sur l'intelligence artificielle et les données*, qui réglemente les « systèmes d'intelligence artificielle » et le traitement des données liées à ces systèmes.

Il convient de souligner que le projet de loi C-27 crée un environnement plus contraignant pour les sociétés qui traitent des renseignements personnels en ajoutant des outils d'application améliorés et élargis et des recours sévères en cas de non-conformité, comme :

- la possibilité pour le Commissariat de recommander, et pour le Tribunal de la protection des renseignements personnels et des données (tribunal constitué en vertu du projet de loi C-27) d'infliger une pénalité de 10 M$ ou, s'il est supérieur, d'un montant égal à 3 % des recettes globales brutes de l'organisation;
- une augmentation considérable des infractions et des amendes pouvant atteindre 25 M$ ou 5 % des recettes globales brutes;
- un droit privé d'action permettant le recours aux tribunaux dans certaines circonstances.

Ces changements visés par le projet de loi C-27 s'inscrivent dans la tendance mondiale du renforcement des lois et règles entourant la protection de la vie privée initiée par l'Union européenne (avec le RGPD), et cadrent avec les changements apportés au niveau provincial au Québec.

Au Québec, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* est entrée en vigueur dans son intégralité en septembre 2024. Communément appelée la « loi 25 », elle a apporté des changements importants aux lois québécoises sur la protection des renseignements personnels dans les secteurs privé et public, entre autres. La loi 25 impose notamment les obligations suivantes aux entreprises établies au Québec :

- désigner un responsable de la protection des renseignements personnels chargé de veiller au respect des lois sur la protection de la vie privée (ce rôle sera attribué à la personne ayant la plus haute autorité dans l'entreprise si elle ne délègue pas cette fonction par écrit à quelqu'un d'autre);
- aviser la Commission d'accès à l'information et les personnes concernées si un incident de confidentialité « présente un risque qu'un préjudice sérieux soit causé »;
- réaliser des évaluations des facteurs relatifs à la vie privée dans diverses situations, notamment avant de traiter certains renseignements personnels dans le cadre de projets technologiques ou avant de communiquer des renseignements personnels à l'extérieur du Québec;
- permettre aux personnes concernées d'exercer de nouveaux droits, notamment le droit à la portabilité des données et le droit à la réindexation;
- payer des amendes d'un montant maximal de 25 000 000 $ CA ou d'un montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice précédent (le montant le plus élevé étant retenu), en cas de non-respect.

Les entreprises ayant des activités au Québec doivent tenir compte de ces dispositions.

### LCAP – Loi canadienne anti-pourriel

L'envoi de messages électroniques commerciaux (MEC) à des adresses électroniques au 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 (la « LCAP ») et par son règlement d'application. Les activités réglementées par la LCAP et par la LPRPDE se chevauchent. Par conséquent, ces deux lois doivent être prises en compte. Pour mieux comprendre les exigences de la LCAP, consultez le chapitre Technologies de ce guide.