LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Par Eugen Miscoi, Jon Adessky et Pierre Dushime

LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Résumé

Toutes les entreprises au Canada sont assujetties aux lois qui régissent la collecte, l'utilisation et la communication de renseignements personnels dans le cours des activités commerciales et, dans certains territoires, dans le cadre de la gestion des employés. Les « renseignements personnels » sont généralement des renseignements concernant une personne identifiable. La collecte, l'utilisation et la communication de renseignements personnels par des entreprises et entités du secteur privé dans les provinces de la Colombie-Britannique, de l'Alberta et du Québec sont régies par la législation édictée par chacune de ces provinces, tandis qu'une loi fédérale sur la protection des renseignements personnels applicable au secteur privé régit la collecte, l'utilisation et la communication des renseignements personnels dans le reste du Canada.

TOUTES LES ENTREPRISES AU CANADA SONT ASSUJETTIES AUX LOIS QUI RÉGISSENT LA COLLECTE, L'UTILISATION ET LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS DANS LE COURS DES ACTIVITÉS COMMERCIALES.

Ces régimes législatifs se fondent de manière générale sur les dix principes suivants qui régissent la collecte, l'utilisation et la communication des renseignements personnels :

— la responsabilité;

— la détermination des fins;

— le consentement;

— la limitation de la collecte;

— la limitation de l'utilisation, de la communication et de la conservation;

— l'exactitude;

— les mesures de sécurité;

— la transparence;

— l'accès aux renseignements personnels; et

— la possibilité de porter plainte.

En plus de leurs lois générales sur la protection des renseignements personnels applicables au secteur privé, les provinces de l'Alberta, du Manitoba, de la Nouvelle-Écosse, du Nouveau-Brunswick, de Terre-Neuve-et-Labrador, de l'Ontario, du Québec et de la Saskatchewan ont également adopté des lois afin de protéger spécifiquement les renseignements personnels sur la santé. Par exemple, la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (Ontario) établit des règles à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels sur la santé par des dépositaires de renseignements sur la santé en Ontario.

Loi fédérale sur la protection des renseignements personnels applicable au secteur privé – LPRPDE

Au niveau fédéral, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) régit la collecte, l'utilisation et la communication de renseignements personnels dans les provinces et dans les territoires qui n'ont pas adopté de législation essentiellement similaire en matière de protection des renseignements personnels, de même que dans le cadre d'activités commerciales interprovinciales et internationales. La LPRPDE s'applique à tous les établissements, entreprises et commerces réglementés par le gouvernement fédéral, peu importe la province dans laquelle ils exercent. Cela inclut notamment les banques, les compagnies aériennes, les prestataires de services de télécommunications et d'autres organisations du ressort fédéral. Comme expliqué plus en détail ci-dessous, si la *Loi sur la protection de la vie privée des consommateurs* (LPVPC) — instaurée par la *Loi édictant la Loi sur la protection de la vie privée des consommateurs*, la *Loi sur le Tribunal de la protection des renseignements personnels et des données* et la *Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois* (Projet de loi C-27) — est adoptée, le régime de protection des renseignements personnels énoncé dans la LPRPDE sera modernisé de façon à correspondre étroitement à la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels du Québec* (Loi 25, auparavant Projet de loi 64).

À moins que certaines exceptions ne s'appliquent, la connaissance et le consentement d'une personne sont nécessaires pour collecter, utiliser ou communiquer ses renseignements personnels. Le consentement explicite peut être nécessaire en ce qui a trait à des renseignements personnels plus délicats (par exemple, des renseignements médicaux ou

financiers), alors que le consentement implicite peut être suffisant pour des renseignements personnels non délicats (par exemple, l'adresse postale). En vertu des modifications apportées à la LPRPDE en 2015, le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce que l'individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti. Des exceptions à l'exigence de consentement, notamment la communication de renseignements personnels dans le cadre de certaines opérations commerciales, sont prévues par la loi.

Les *Lignes directrices pour l'obtention d'un consentement valable* (Lignes directrices) du Commissariat à la protection de la vie privée (CPVP) précisent que le fait de ne pas obtenir un consentement valable peut conduire une entreprise à perdre sa capacité à gérer les renseignements personnels nécessaires à son fonctionnement. Afin de favoriser l'obtention d'un consentement valable, les sociétés sont encouragées à : i) s'assurer que leur politique en matière de protection des renseignements est rédigée en langage clair; ii) utiliser des avis « juste-à-temps » sur leur site Web comme complément à la version longue de la politique en matière de protection des renseignements; iii) rédiger un résumé des principaux points à mettre au début de la politique en matière de protection des renseignements; et à iv) utiliser des outils interactifs dans la présentation de l'information concernant la protection des renseignements.

Lois provinciales sur la protection des renseignements personnels

L'Alberta, la Colombie-Britannique et le Québec ont adopté leurs propres lois sur la protection des renseignements personnels applicable au secteur privé pouvant s'appliquer à la place de la LPRPDE aux pratiques d'entreprises et d'entités situées dans ces provinces en matière de protection des renseignements personnels des consommateurs ainsi que des salariés. Ces lois sont, en substance, jugées de manière similaire à la LPRPDE. La partie suivante donnera donc une vue d'ensemble du régime de protection des renseignements personnels du Québec, en se concentrant uniquement sur cette province parce qu'elle établit certaines des exigences les plus strictes applicables au Canada. En d'autres termes, se conformer au régime de protection des renseignements personnels du Québec permet d'être en conformité substantielle avec les autres régimes de protection des renseignements personnels du pays.

Québec

La *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi québécoise) s'applique à la collecte, à l'utilisation ou à la communication de renseignements personnels sur le territoire de la province par « toute personne qui exploite une entreprise ». Ce régime de protection des renseignements personnels a été modifié par la Loi 25, et continue de l'être. Le tableau 1 ci-dessous résume les nouvelles obligations principales imposées par la Loi 25, qui sont classées en fonction de leur date d'entrée en vigueur.

Tableau 1 : Sommaire et dates d'entrée en vigueur des modifications

22 septembre 2022 :

Nouvelles obligations

- Nomination d'un responsable de la protection des renseignements personnels
- Déclaration des atteintes à la protection des données
- Exceptions au consentement pour les :
  - transactions commerciales;
  - études, recherches ou productions de statistiques
- Communication de bases de données biométriques pour l'authentification à la Commission d'accès à l'information (CAI) du Québec

22 septembre 2023 :

Nouvelles obligations

- Cadre pour la protection des renseignements personnels
- Exigences supplémentaires en matière de transparence
- Évaluations des facteurs relatifs à la vie privée
- Protection des renseignements personnels par défaut et dès la conception
- Droits de désindexation
- Exigences supplémentaires en matière de consentement
- Transferts transfrontaliers de renseignements personnels
- Nouveau régime pour l'utilisation secondaire de renseignements personnels
- Obligations strictes de conservation et de destruction
- Nouvelle obligation lorsqu'une décision automatisée est prise à l'aide des renseignements personnels d'un individu
- Nouveau régime pour les coordonnées professionnelles
- Nouvelles sanctions en cas de non-conformité

22 septembre 2024 :

Nouvelles obligations

- Droit à la portabilité des données

Les amendes qui pourraient résulter du non-respect de la Loi québécoise constituent une évolution importante apportée par la Loi 25. En cas de non-respect et à compter du 22 septembre 2023, la CAI pourra imposer une sanction administrative pécuniaire pouvant aller jusqu'à 10 000 000 $ CA ou jusqu'au montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé. La CAI peut également intenter des poursuites pénales éventuellement assorties d'amendes pouvant aller jusqu'à 25 000 000 $ CA ou jusqu'au montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé. En cas de récidive, les amendes peuvent être doublées. Le **Cadre général d'application des sanctions administratives pécuniaires** de la CAI détermine les amendes initiales pour différents niveaux de manquement, ce qui permet de classer la gravité du manquement en quatre catégories : mineur, modéré, grave et très grave. Cette catégorisation détermine la sanction de base. Ensuite, la CAI ajuste le montant de base en fonction de facteurs tels que la nature du manquement, le risque de préjudice et la sensibilité des renseignements. Cependant, les montants de base ne constituent pas un plancher, et donc peuvent être inférieurs en présence de facteurs atténuants. Toutefois, les amendes peuvent augmenter considérablement en présence de facteurs aggravants, jusqu'à 10 000 000 $ CA ou jusqu'au montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent d'une entreprise ou entité si ce dernier montant est plus élevé.

Principales tendances des lois canadiennes sur la protection des renseignements personnels

Avis des atteintes à la protection des renseignements personnels et tenue de registres

Pendant de nombreuses années, la *Personal Information Protection Act de l'Alberta* (PIPA de l'Alberta) était la seule loi sur la protection des renseignements personnels de portée générale applicable au secteur privé au Canada qui imposait aux organisations du secteur privé l'obligation de signaler les atteintes à la protection des renseignements personnels. En vertu de la PIPA de l'Alberta, les organisations du secteur privé ne doivent signaler (à l'Information and Privacy Commissioner de l'Alberta) que les atteintes à la protection des renseignements personnels qui pourraient poser un risque réel de préjudice important pour un individu. L'Information and Privacy Commissioner de l'Alberta décide ensuite si une organisation doit aviser les personnes visées.

Depuis le 1er novembre 2018, en raison des modifications apportées à la LPRPDE en vertu de la *Loi sur la protection des renseignements personnels numériques*, les organisations partout au Canada doivent se conformer à de nouvelles obligations selon les règles en matière d'avis des atteintes. Les organisations assujetties à la LPRPDE ont des obligations en matière de déclaration, d'avis et de conservation de registres pour toute atteinte aux mesures de sécurité. Une atteinte aux mesures de sécurité peut être définie au sens large comme : la « communication non autorisée ou la perte de renseignements personnels, ou les accès non autorisés à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation ». Les obligations de déclaration et d'avis sont déclenchées par la présence d'un risque réel de préjudice grave (RRPG) à un individu. Le RRPG a également une définition générale qui comprend : « la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles ». Les éléments servant à établir si une atteinte aux mesures de sécurité présente un RRPG incluent le degré de sensibilité des renseignements personnels en cause, ainsi que la probabilité que les renseignements personnels aient été utilisés abusivement ou soient en train ou sur le point de l'être.

Le rapport d'atteinte doit être soumis au CPVP « dès que possible après que l'organisation a conclu qu'il y a eu atteinte ». Le même critère s'applique pour remettre aux individus des avis concernant les atteintes qui visent leurs renseignements personnels, sauf si la loi le prévoit autrement. L'avis doit être apparent et contenir suffisamment d'information pour aider les individus touchés à atténuer les risques de préjudice. On peut trouver de l'information sur les renseignements à inclure dans les rapports écrits soumis au CPVP et les avis aux individus dans le *Règlement sur les atteintes aux mesures de sécurité*. Par ailleurs, qu'il y ait un RRPG ou non, une organisation doit tenir un registre d'atteinte à la sécurité pour une période de 24 mois suivant une atteinte aux mesures de sécurité. Pendant cette période, les organisations doivent accéder en tout temps aux demandes d'accès au registre du CPVP. De plus, l'organisation qui subit une atteinte devra aviser toute autre organisation ou toute institution gouvernementale si elle croit que celle-ci peut être en mesure de réduire le risque de préjudice pouvant résulter de l'atteinte.

Les organisations assujetties à la LPRPDE sont tenues responsables si elles contreviennent sciemment aux exigences d'avis. Une organisation

peut donc s'exposer à des amendes pouvant aller jusqu'à 100 000 $ CA par infraction. De plus, la LPRPDE confère au commissaire à la protection de la vie privée du Canada le droit de rendre publique toute information dont il a connaissance dans le cadre de l'exercice de ses devoirs ou de ses pouvoirs, de même que de rendre public le contenu des rapports de déclaration d'atteinte à la sécurité soumis au CPVP, s'il juge que l'information est d'intérêt public. Dans l'ensemble, ces dispositions imposent des obligations plus strictes en matière de protection des renseignements personnels, de consentement et de déclaration d'atteinte à la sécurité.

Au Québec, la Loi 25 a mis en place de nouvelles obligations en matière d'avis aux entreprises du secteur privé qui subissent une atteinte à la protection de renseignements personnels, ce que la Loi 25 appelle un « incident de confidentialité ». Un incident de confidentialité est défini comme l'accès, l'utilisation ou la communication non autorisés de renseignements personnels, la perte de renseignements personnels ou toute atteinte à la protection de ces renseignements. En cas d'incident de confidentialité présentant un « risque de préjudice sérieux », les entreprises sont tenues de prendre des mesures raisonnables pour atténuer le risque et prévenir des incidents similaires. Plusieurs facteurs sont à prendre en compte pour savoir si un incident donné présente un « risque de préjudice sérieux », notamment la sensibilité des renseignements concernés, les possibles conséquences de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables. S'il existe un « risque de préjudice sérieux », les organisations sont obligées d'aviser, avec diligence, aussi bien la CAI que les personnes exposées au risque.

Transferts transfrontaliers de renseignements

En ce qui concerne les transferts de renseignements personnels aux fournisseurs de services situés à l'extérieur du Canada, les organismes fédéraux de réglementation en matière de protection des renseignements personnels considèrent que le principe de « transparence » prévu dans la LPRPDE exige qu'un avis de tels transferts doive être transmis aux personnes concernées. La PIPA de l'Alberta exige que les organisations avisent les personnes dont les renseignements personnels sont transférés à un fournisseur de services situé à l'extérieur du Canada. Au Québec, à compter du 22 septembre 2023, la Loi 25 prévoit de nouvelles obligations pour les entreprises prenant part au transfert transfrontalier de renseignements personnels. Au moment de la collecte des renseignements et sur demande, celles-ci doivent informer les

personnes concernées de la possibilité que les renseignements recueillis soient communiqués à l'extérieur du Québec. Avant de communiquer des renseignements personnels à l'extérieur du Québec, une évaluation des facteurs relatifs à la vie privée doit être effectuée afin d'établir que les renseignements transférés bénéficieront d'une protection adéquate dans l'État où ces renseignements seront transférés. L'évaluation prend en compte des facteurs tels que la sensibilité des renseignements, les fins, les mesures de protection et le régime juridique de l'État destinataire. Les transferts transfrontaliers doivent également faire l'objet d'une entente écrite qui tient compte des résultats de l'évaluation et des conditions convenues pour atténuer les risques. Il convient de noter que ces exigences s'appliquent de la même manière aux transferts de renseignements personnels interprovinciaux et internationaux.

Lignes directrices pour les entreprises

Que la LPRPDE ou une loi provinciale similaire constitue le régime de protection des renseignements personnels applicable, les priorités immédiates pour la plupart des sociétés qui établissent une entreprise au Canada devraient être les suivantes :

— définir une stratégie documentée d'observation des lois sur la protection des renseignements personnels qui précise les normes à respecter eu égard au régime législatif applicable;

— adopter une politique en matière de protection des renseignements personnels externe et interne et des pratiques de gestion des renseignements personnels pour s'assurer de respecter les lois sur la protection des renseignements personnels applicables;

— désigner une personne qui sera responsable d'administrer et de superviser les pratiques de gestion des renseignements personnels de la société et qui apportera tous les changements nécessaires en vertu de la loi applicable;

— passer en revue les pratiques actuelles de la société en matière de gestion des renseignements personnels à l'extérieur du Canada et les pratiques proposées en matière de gestion des renseignements à l'intérieur du Canada, notamment déterminer la nature des renseignements personnels recueillis, l'endroit où ils sont recueillis, les consentements à obtenir et les fins auxquelles les renseignements personnels sont recueillis, l'endroit où ils sont conservés, la façon dont ils sont utilisés et à quel moment et à qui ils sont communiqués, et la manière dont les pratiques actuelles de la société en matière de

gestion des renseignements personnels peuvent devoir être modifiées quant à la collecte, à l'utilisation et à la divulgation des renseignements personnels au Canada;

— examiner l'infrastructure de gestion des données de la société pour s'assurer qu'elle est suffisamment souple et robuste pour permettre la mise en œuvre des politiques relatives à la protection des renseignements personnels et des pratiques de gestion des données de la société;

— insérer les consentements obligatoires dans les contrats, les formulaires (y compris les formulaires Web) et les autres documents qui sont utilisés lors de la collecte de renseignements personnels auprès de personnes (clients et employés);

POUR LA PLUPART DES SOCIÉTÉS QUI ÉTABLISSENT UNE ENTREPRISE AU CANADA, LES PRIORITÉS IMMÉDIATES DEVRAIENT COMPRENDRE LA DÉSIGNATION D'UNE PERSONNE QUI SERA RESPONSABLE DE L'ADMINISTRATION ET DE LA SUPERVISION DES PRATIQUES DE GESTION DES RENSEIGNEMENTS PERSONNELS DE LA SOCIÉTÉ.

— examiner les ententes pour garantir, en ce qui concerne les contrats conclus avec des tiers auxquels des renseignements personnels seront communiqués (ou lorsque le tiers aura accès aux renseignements personnels), que le tiers s'engage à respecter les modalités contractuelles appropriées, notamment préciser la propriété des données et veiller à ce que le tiers fournisse des mesures de protection adéquates des renseignements; s'assurer que les renseignements personnels seront utilisés aux seules fins pour lesquelles ils ont été communiqués au tiers; veiller à ce que le tiers cesse d'utiliser (ou retourne ou détruise) les renseignements personnels sur demande; et prévoir l'indemnisation par le tiers quant à tout manquement à ces modalités.

— effectuer des évaluations des facteurs relatifs à la vie privée pour examiner correctement les risques pour les renseignements personnels en lien avec de nouveaux projets et des transferts transfrontaliers de renseignements; et

— adopter un plan d'intervention en cas d'atteinte à la protection des renseignements qui indique clairement les personnes-ressources internes et les conseillers externes à contacter. Un tel plan permettra d'éviter les erreurs et d'obtenir du soutien immédiat en cas d'incident. Une organisation doit être en mesure de déceler rapidement

une atteinte à la protection des renseignements, de procéder immédiatement à l'exécution du plan d'intervention, d'isoler les systèmes touchés, d'évaluer les dommages et de corriger la situation.

Ces premières étapes peuvent nécessiter plusieurs mois, selon la taille et la maturité de la société.

Cas d'inobservation

Il faut tenir compte du respect des lois sur la protection des renseignements personnels dans le cadre de toute opération commerciale touchant la communication ou le transfert de renseignements personnels, comme les achats ou les ventes d'entreprises, les opérations d'impartition et les opérations de titrisation. Par exemple, lorsqu'on envisage d'acheter une entreprise canadienne, il est crucial d'inclure un examen des politiques et pratiques en matière de protection des renseignements personnels de la société cible dans le cadre du contrôle préalable. Si des renseignements personnels sur les employés ou les clients doivent être communiqués à l'acheteur dans le cadre du contrôle préalable, il est également essentiel qu'un régime de confidentialité approprié soit établi pour le processus. Il est recommandé que seuls les renseignements personnels nécessaires à l'opération ou à ses modalités (y compris le prix), ou susceptibles d'avoir une incidence sur la décision d'aller de l'avant avec l'opération soient communiqués.

Le défaut de se conformer aux lois sur la protection des renseignements personnels peut mener à des plaintes devant le commissaire à la protection de la vie privée compétent, à des ordonnances et à des amendes. Une entreprise dont les pratiques en matière de protection des renseignements personnels sont déficientes peut faire l'objet de mauvaise presse en raison du défaut de se conformer aux lois sur la protection des renseignements personnels.

La Loi 25 introduit de nouvelles conséquences au non-respect de la loi pour les entreprises exerçant des activités au Québec. Voir **Québec**.

Étant donné la complexité des lois sur la protection des renseignements personnels et les différences entre les diverses lois qui peuvent s'appliquer à une société ou à une unité d'exploitation particulière, il peut être difficile pour une entreprise de s'assurer de sa conformité avec les lois sur la protection des renseignements personnels à tous les échelons, en particulier s'il s'agit d'une entreprise active à l'échelle internationale.

Il est important de noter que les exceptions à l'exigence de consentement en cas de situation d'urgence peuvent varier selon les lois canadiennes sur la protection des renseignements personnels et peuvent être assorties de certaines conditions. En général, la personne concernée doit, si possible, être avisée de la communication avant celle-ci ou sans délai après. En outre, ces autorisations législatives ne s'appliquent pas toujours aux opérations commerciales « normales ». Les sociétés sont donc encouragées à tenir compte des lois applicables avant de mettre en œuvre les autorisations législatives qui prévoient des exemptions à l'obligation d'obtenir le consentement pour la collecte, l'utilisation et la communication de renseignements personnels. Enfin, la pandémie de COVID-19 a également suscité des inquiétudes concernant la sécurité des renseignements, en particulier dans le cadre du télétravail. En vue de respecter leurs obligations en matière de protection des renseignements personnels, les sociétés doivent prendre toutes les mesures raisonnables pour s'assurer que les renseignements personnels sont protégés de manière appropriée contre le vol, la perte, la communication non autorisée et d'autres formes de menace.

Modifications en cours et avenir du régime canadien de protection des renseignements personnels

Le gouvernement fédéral et les gouvernements provinciaux du Canada ont présenté des projets de loi et adopté des lois visant à moderniser le paysage de la protection des renseignements personnels là où ils ont compétence.

— Au niveau fédéral, le projet de loi C-27 vise à moderniser le régime fédéral de protection des renseignements personnels. Le projet de loi C-27 créé trois nouvelles lois : (i) la LPVPC, qui remplace les sections sur la protection des renseignements de l'actuelle loi fédérale sur la protection des renseignements personnels applicable au secteur privé, la LPRPDE; (ii) la *Loi sur le Tribunal de la protection des renseignements personnels et des données* (LTPRPD), qui constituerait un tribunal d'appel pour statuer sur les décisions en matière de protection des renseignements en vertu de la LPVPC; et (iii) la *Loi sur l'intelligence artificielle et les données* (LIAD), qui serait la première loi au Canada à réglementer directement l'intelligence artificielle. Le projet de loi C-27 suit le processus législatif fédéral et est susceptible d'évoluer avant que ses trois nouvelles lois ne soient sanctionnées (si elles le sont).

— Au niveau provincial, la Loi québécoise a été remaniée par la Loi 25. La loi 25 a reçu la sanction royale le 22 septembre 2021 et modifie considérablement le régime de protection des renseignements personnels du Québec grâce à une entrée en vigueur, à l'européenne, en trois phases de son cadre, les 22 septembre 2022, 2023 et 2024.

Ces efforts de modernisation s'inscrivent dans le contexte d'un mouvement mondial plus large en faveur d'obligations toujours plus grandes en matière de protection des renseignements personnels pour les sociétés qui collectent et traitent des renseignements personnels dans le cadre de leurs activités. Pour recevoir des conseils pratiques sur la façon efficace de rester au fait de toutes les exigences applicables au Canada, vous pouvez communiquer avec notre groupe multidisciplinaire Cyber/Données.

POUR EN SAVOIR PLUS,
VEUILLEZ COMMUNIQUER AVEC L'UNE DES PERSONNES SUIVANTES :

Charles S. Morgan
cmorgan@mccarthy.ca
514-397-4230

Dan Glover
dglover@mccarthy.ca
416-601-8069