Borden Ladner Gervais

Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : **incidences sur les entreprises**

Juin 2022

Le 15 juin 2022, le Ministre de l'Innovation, des Sciences et de l'Industrie a déposé le projet de loi C-27, *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* (ou *Loi de 2022 sur la mise en œuvre de la Charte du numérique*). Ce projet de loi tant attendu succède au projet de loi C-11, déposé en 2020, qui fut abandonné suite au déclenchement des élections fédérales en août 2021 (« **C-11 (2020)** »).

Le projet de loi C-27 réintroduit ainsi deux lois qui vont sembler familières à ceux qui ont suivi le projet de loi C-11 (2020), soit la *Loi sur la protection de la vie privée des consommateurs* (« **LPVPC** ») et la *Loi sur le Tribunal de la protection des renseignements personnels et des données*. La principale nouveauté du projet de loi C-27 tient dans l'introduction d'une troisième loi, la *Loi sur l'intelligence artificielle et les données* (« **LIAD** »).

Le projet de loi C-27 vise à remplacer la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDÉ** ») par un cadre juridique modernisé qui soit plus adapté à l'ère numérique. Ce bulletin présente les principales différences entre la législation proposée et le régime fédéral actuel de protection des renseignements personnels dans le secteur privé régi par la LPRPDÉ.

Table des matières

Ce que vous devez savoir

Le présent article dresse un aperçu des éléments clés de la LPVPC ainsi que de leur incidence sur les entreprises canadiennes.

Tel que plus amplement décrit dans ce bulletin, la LPVPC propose un nouveau régime de protection des renseignements personnels qui introduirait plusieurs changements déjà proposés par son prédécesseur, le projet de loi C-11 (2020):

- Nouveaux mécanismes de pénalités :
    - Attribution au *Tribunal de la protection des renseignements personnels et des données* nouvellement constitué le pouvoir d'imposer, sur recommandation du Commissariat à la protection de la vie privée du Canada, des sanctions administratives pécuniaires d'un montant pouvant aller jusqu'à 10 000 000 $ CA ou 3 % des recettes globales brutes de l'organisation au cours de son exercice précédent, selon le plus élevé des deux montants.
    - Augmentation des amendes susceptibles d'être imposées dans le cadre de poursuites pénales jusqu'à un montant maximum de 25 000 000 $ CA, ou, s'il est supérieur, à un montant correspondant à 5 % des recettes globales brutes de l'organisation au cours de son exercice précédent.
    - Nouveau recours civil, le « droit privé d'action », pour les particuliers.
    - Nouvelles dispositions permettant la création de « codes de pratique » et de « programmes de certification ».
- Nouveaux droits individuels inspirés du droit européen : droit d'être informé des décisions automatisées, droit de retrait et droit à la mobilité.
- Règles de responsabilité renforcées :
    - Nouvelle définition de la notion de « relève ».
    - Nouvelle obligation d'établir, de mettre en œuvre et de rendre disponible un programme de gestion de la protection des renseignements personnels.
    - Clarification du rôle et des responsabilités des fournisseurs de services.
- Exigences renforcées en matière de consentement et une clarification de la notion de consentement valide.
- Accomplissement de certaines règles : nouvelles exceptions au consentement concernant les renseignements dépersonnalisés et les pratiques commerciales légitimes.

La nouvelle version de la LPVPC (C_27) propose également des changements par rapport à son prédécesseur, le projet de loi C-11 (2020). Pour vous aider à analyser le projet de loi C-27, nous avons préparé un tableau décrivant les principales nouveautés du projet de loi C-27 par rapport au projet de loi C-11 (2020). Nous avons en outre résumé ces changements clés au début de chaque section.

Introduction

La proposition du gouvernement fédéral de moderniser la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDÉ** ») – une loi adoptée il y a près de vingt ans – est tout aussi ambitieuse que prudente dans sa tentative d'améliorer de manière significative la protection des renseignements personnels des individus. La proposition, qui remplacerait les dispositions de la LPRPDÉ relatives à la protection des renseignements personnels par la *Loi sur la protection de la vie privée des consommateurs* (la « **LPVPC** »), vise à rendre opérationnelle la Charte canadienne du numérique de même que les propositions antérieures visant à renforcer la protection de la vie privée dans l'ère numérique afin de relever les défis posés par l'économie numérique et les nouvelles technologies. La principale nouveauté du projet de loi C-27 tient dans l'introduction d'une troisième loi, la Loi sur l'intelligence artificielle et les données (« **LIAD** »). Autrement, la proposition est relativement similaire au projet de loi C-11 (2020) en ce qu'elle promulguerait la *Loi sur le Tribunal de la protection des renseignements personnels et des données*, établissant un nouveau *Tribunal de la protection des renseignements personnels et des données* (le « **Tribunal** »), qui aurait la capacité d'imposer des pénalités importantes. De plus, les violations les plus graves de la LPVPC pourraient donner lieu, en cas de poursuites, à des amendes ayant été décrites parmi les plus sévères des lois sur la protection des renseignements personnels du G7, y compris le *Règlement général sur la protection des données* (le « **RGPD** ») de l'Union européenne et le *California Consumer Privacy Act of 2018* (la « **CCPA** »).

Bien qu'elle s'inspire clairement d'initiatives similaires dans d'autres pays, à savoir le RGPD de l'UE et la CCPA de Californie, la proposition canadienne est unique dans son approche en ce qu'elle offre aux entreprises, dans de nombreux cas, une souplesse et une clarté accrues par rapport aux exigences du régime actuel de protection des renseignements personnels. Plus particulièrement, elle codifie plusieurs directives et les décisions antérieures du Commissariat à la protection de la vie privée du Canada (le « **Commissaire** ») et offre aux individus de nouveaux droits plus étroitement encadrés que ceux qui sont actuellement prévus par le RGPD. En ce sens, il convient de noter qu'à plusieurs égards la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (« **Loi sur le secteur privé du Québec** ») telle que modifié par l'adoption du projet de loi 64 (« **Loi 64** »), est considérablement plus contraignant que la LPVPC, ce qui pourrait soulever un certain nombre de défis du point de vue de l'interopérabilité pour les entreprises qui exercent leurs activités à l'échelle nationale. Pour une analyse plus détaillée des modifications proposées par le projet de Loi 64 du Québec, veuillez consulter notre Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé.

Les différences entre la Loi 64 du Québec et la LPVPC soulignent l'importance de renforcer la cohérence entre les différents régimes de protection des renseignements personnels, d'autant plus que le statut d'adéquation du Canada dans le cadre du RGPD, qui confère un avantage concurrentiel aux entreprises canadiennes traitant des données personnelles assujetties au RGPD, doit être renouvelé. En outre, on peut s'attendre à une éventuelle réforme de la loi albertaine sur la protection des renseignements personnels (*Personal Information Protection Act*) (la « **PIPA de l'Alberta** ») et de la loi équivalente en Colombie-Britannique (*Personal Information Protection Act*) (la « **PIPA de Colombie-Britannique** ») qui, avec la Loi sur le secteur privé du Québec, sont toutes trois considérées comme « essentiellement similaires » à la LPRPDÉ et s'appliquent donc en lieu et place de celle-ci pour les questions

intraprovinciales relatives à la protection des renseignements personnels. En effet, en décembre 2021, un comité spécial de l'assemblée législative de la Colombie-Britannique a déposé un rapport recommandant des modifications majeures à la PIPA de Colombie-Britannique (voir « *Special committee recommendations to modernize B.C.'s private sector privacy law* » pour plus de détails – en anglais seulement). De même, en juin 2021, le gouvernement de l'Ontario a publié un livre blanc intitulé Modernisation de la protection de la vie privée en Ontario, qui contient plusieurs propositions pour l'adoption d'une première loi sur la protection des renseignements personnels dans le secteur privé pour cette province (voir « *L'Ontario va de l'avant avec une proposition de réforme législative en matière de protection de la vie privée* »).

Mise en œuvre

Mise en oeuvre – Résumé des changements de C-27 par rapport à C-11 (2020)

- Changements procéduraux par rapport aux enquêtes du Commissaire (arts. 83, 84, 85).
- **Changement important** → Les contraventions à de nouvelles dispositions peuvent mener à des pénalités, soit: (i) programme de gestion de la protection des renseignements personnels (art. 9), (ii) transferts aux fournisseurs de services (art. 11), (iii) établissement des fins et fin nouvelle (art. 12(3) and (4)), (iv) obligation d'obtenir le consentement (art. 15(1)), (v) interdiction d'obliger le consentement lorsque le renseignement n'est pas nécessaire (art. 15(7), (vi) consentement obtenu par subterfuge (art. 16), (vii) retrait du consentement (art. 17(2)), (viii) conservation (s. 53), (ix) obligation des fournisseurs de services d'informer l'organisation lors d'une atteinte aux mesures de sécurité (art. 61), (x) rendre disponible des renseignements à propos de ses politiques et pratiques (art. 62(1)). (art. 94(1)).
- **Changement important** → Le Commissaire doit prendre en compte de nouveaux facteurs dans sa décision de recommander que le Tribunal impose une pénalité: (i) la preuve que l'organisation a pris toutes les précautions voulues pour empêcher la contravention; (ii) les efforts raisonnables que l'organisation a déployés pour atténuer ou neutraliser les incidences de la contravention; (iii) tout élément prévu par règlement. (art. 94(2)).
- Le pouvoir du Commissaire d'auditer les pratiques de l'organisation en matière de protection des renseignements personnels s'étend aux situations dans lesquelles il a des motifs raisonnables de croire qu'elle contrevient ou est susceptible de contrevenir à la LPVPC. (art. 97).

La LPVPC introduit des changements majeurs en matière d'application de la législation fédérale sur la protection des renseignements personnels, ce qui créera de nouveaux risques de non-conformité pour les organisations.

Plus particulièrement, la LPVPC confère de nouveaux pouvoirs d'ordonnance au Commissaire. Ce dernier sera également en mesure d'émettre des recommandations au Tribunal pour l'imposition de pénalités pouvant atteindre 10 000 000 $ ou 3 % des recettes globales brutes de l'organisation, selon le montant le plus élevé. Par contraste, soulignons que le montant des pénalités administratives en vertu du RGPD et de la Loi 64 au Québec est plafonné à 2 %. En outre, les infractions les plus graves à la LPVPC constitueraient des infractions punissables d'une amende pouvant atteindre jusqu'à 25 000 000 $ CA ou 5 % des recettes globales brutes de l'organisation. Encore une fois, il s'agit d'une limite supérieure à celle actuellement prévue par le RGPD et la Loi 64 du Québec, où le plafond est fixé à 4 % (notons que la Loi 64 du Québec prévoit que le montant des amendes peut être doublé en cas de récidive).

Pouvoirs du Commissaire

Pouvoirs actuels – enquêtes, accords de conformité et audits. La LPVPC reprend certains pouvoirs prévus dans la LPRPDÉ, notamment la possibilité pour les particuliers de déposer des plaintes et la possibilité pour le Commissaire de prendre lui-même l'initiative d'une plainte (article 82 LPVPC remplaçant l'article 11 LPRPDÉ). Le Commissaire conserve également les pouvoirs suivants :

- Faire enquête sur toute plainte reçue (art. 83 LPVPC remplaçant l'art. 12 LPRPDÉ);
- Conclure des accords de conformité avec les organisations ayant contrevenu à la loi (art. 87 LPVPC remplaçant l'art. 17.1 LPRPDÉ);
- Mener des vérifications concernant le respect de la loi par les organisations (art. 97 LPVPC remplaçant l'art. 18 LPRPDÉ).

Nouveaux pouvoirs – ordonnances de conformité et recommandations de pénalité. La LPVPC accorde toutefois au Commissaire de nouveaux pouvoirs lui permettant de mener une enquête après avoir examiné une plainte (art. 89) ou en cas de non-respect d'un accord de conformité (art. 90). Au terme d'une enquête, le Commissaire doit rendre une décision dans laquelle, il peut émettre une ordonnance de conformité (art. 93).

- **Ordonnances de conformité**. La LPVPC confère au Commissaire d'importants nouveaux pouvoirs, dont celui d'ordonner aux organisations de faire ce qui suit :
    - prendre des mesures afin de se conformer à la loi;
    - cesser toute action qui contrevient à la loi;
    - de respecter une entente de conformité;
    - rendre publiques toutes les mesures visant à corriger ses politiques, pratiques ou procédures (art. 93(2)).

Une organisation pourra interjeter appel d'une ordonnance de conformité auprès du Tribunal, tel qu'il est discuté ci-dessous. Toutefois, si l'ordonnance ne fait pas l'objet d'un appel, elle sera exécutoire de la même manière qu'une ordonnance de la Cour fédérale (art. 104).

- **Recommandation de pénalité**. Le Commissaire doit également décider s'il recommande au Tribunal d'imposer une pénalité en cas de violation de certaines dispositions clés de la LPVPC (art. 94). Or, contrairement à d'autres commissaires à la protection de la vie privée (par exemple, les autorités de contrôle sous le RGPD et la Commission d'accès à l'information au Québec), le Commissaire n'a pas le pouvoir d'imposer directement des pénalités aux organisations en cas de violation de la LPVPC.

Pénalités monétaires imposées par le Tribunal

La LPVPC confère au Tribunal le pouvoir d'imposer une pénalité à une organisation après avoir laissé à celle-ci et au Commissaire la possibilité de présenter leurs observations (art. 95(1)). Le Tribunal doit se fonder sur les conclusions du Commissaire ou sur ses propres conclusions dans le cas d'un appel (art. 95 (2)). Fait important à noter, les organisations pourront invoquer une défense de diligence raisonnable (art. 95(3)).

La pénalité maximale pour l'ensemble des contraventions identifiées correspond est de 10 000 000 $ ou 3 % des recettes globales brutes de l'organisation au cours de son exercice précédent celui pendant lequel

la pénalité est infligée, selon le montant le plus élevé (art. 95(4)). La LPVPC prévoit les facteurs dont le Tribunal doit tenir compte pour établir le montant de la pénalité (art. 95(5)).

Appels devant le Tribunal

La LPVPC prévoit également que les plaignants et les organisations visées par une décision du Commissaire peuvent porter la décision en appel devant le Tribunal (art. 101). Ce droit s'étend également à toute ordonnance de conformité émise par le Commissaire contre l'organisation et à toute décision émise par le Commissaire dans laquelle il décide de ne pas recommander l'imposition d'une sanction. Les décisions du Tribunal sont définitives et exécutoires, sous réserve de leur contrôle judiciaire par la Cour fédérale.

Infractions et peines

Les violations les plus graves de la LPVPC constituent une infraction passible d'une amende maximale de 25 000 000 $ ou de 5 % des recettes globales brutes de l'organisation au cours de son exercice précédent celui pendant lequel l'amende est infligée (art. 128). Comme dans le cas des infractions prévues à l'article 28 de la LPRPDÉ, les poursuites seront intentées par le procureur général du Canada. Les violations suivantes constituent une infraction au sens de l'article 128 LPVPC :

- contrevenir sciemment aux exigences de déclaration et d'avis en cas d'atteinte aux mesures de sécurité en lien avec des renseignements personnels (art. 58) ou encore aux exigences de tenue de registre à la suite d'une telle atteinte (art. 60(1));
- contrevenir sciemment à l'obligation de conserver les renseignements personnels faisant l'objet d'une demande d'accès (art. 69);
- utiliser sciemment des renseignements dépersonnalisés pour identifier une personne (art. 75);
- contrevenir sciemment à une ordonnance de conformité rendue par le Commissaire;
- entraver l'action du Commissaire dans le cadre d'une vérification, d'une enquête ou de l'examen d'une plainte.

Droit privé d'action

La LPVPC introduit un nouveau droit privé d'action permettant à un individu touché par une violation à la LPVPC d'intenter une action contre l'organisation en vue d'obtenir des dommages-intérêts pour la perte ou le préjudice causé par la violation, à condition :

- que le Commissaire conclue que l'organisation a enfreint la LPVPC et que sa décision ne puisse plus faire l'objet d'un appel, soit parce que le délai d'appel a expiré, soit parce que le Tribunal a rejeté un appel antérieur; ou
- que le Tribunal estime que l'organisation a enfreint la LPVPC.

La LPVPC prévoit également un droit privé d'action pour les individus lorsqu'une organisation a été sanctionnée pour une infraction à la LPVPC (par exemple, le défaut de faire les déclarations requises au Commissaire, le défaut de tenir des dossiers ou de conserver certains renseignements, le fait de pénaliser un employé pour avoir signalé une infraction à la LPVPC ou l'utilisation de renseignements dépersonnalisés pour

identifier une personne). Les individus touchés par l'action ou l'omission ayant mené à l'infraction peuvent intenter une poursuite en réparation du préjudice subi.

Dans chaque cas, le délai de prescription applicable est de deux ans suivant la date de la recommandation par le Commissaire, la décision du Tribunal ou la condamnation pour une infraction à la LPVPC (selon le cas).

Le droit privé d'action prévu dans la LPVPC semble considérablement plus large que celui prévu dans la Loi 64 au Québec, puisque ce dernier se limite à une attribution de dommages punitifs d'au moins 1 000 $ en cas de faute lourde ou intentionnelle.

Dispositions relatives à la dénonciation et à la protection contre les représailles

La LPVPC maintient la protection des dénonciateurs qui figure actuellement dans la LPRPDÉ (art. 126 LPVPC remplaçant l'art. 27 LPRPDÉ). Le Commissaire a d'ailleurs utilisé à au moins une occasion des renseignements reçus en vertu de cette disposition pour initier une enquête (Résumé de conclusions d'enquête en vertu de la LPRPDÉ no 2005-310). La LPVPC comprend également une disposition anti-représailles similaire à celle prévue actuellement dans la LPRPDÉ (l'art. 127 LPVPC remplaçant l'art. 27.1 LPRPDÉ).

Codes de pratique et programmes de certification

Les articles 76 et 77 de la LPVPC introduisent de nouvelles dispositions permettant la création de « codes de pratique » et de « programmes de certification », un moyen d'encourager les pratiques volontaires et sectorielles qui favorisent la protection des renseignements personnels. Des dispositions similaires sont incluses dans les articles 40 à 43 du RGPD et pourraient guider l'application de la LPVPC.

Afin d'encourager le développement de saines pratiques en matière de respect de la vie privée, la LPVPC permet à toute organisation (soumises ou non à la LPVPC, y compris les institutions gouvernementales) de demander l'approbation de ses codes de pratique et de ses programmes de certification par le Commissaire. Notons que cette pratique ne constituera pas nécessairement une preuve de conformité à la LPVPC. Toutefois, le Commissaire aura le pouvoir discrétionnaire de refuser d'enquêter auprès des organisations certifiées (art. 83(1)(d)) et il lui est interdit de recommander qu'une pénalité soit imposée à une organisation « si le Commissaire est d'avis qu'au moment de la contravention de la disposition en cause l'organisation se conformait aux exigences d'un programme de certification qu'il a approuvé » (art. 94(3) LPVPC). Une organisation peut choisir de se conformer volontairement et de maintenir la certification comme un moyen de réduire les risques de non-conformité à la LPVPC et souligner son engagement à respecter la vie privée des consommateurs.

Responsabilité

Responsabilité – Résumé des changements de C-27 par rapport à C-11 (2020)

- **Changement important** → Nouveaux pouvoirs permettant au Commissaire de fournir des conseils ou recommander des mesures correctives à l'organisation relativement à son programme de gestion des renseignements personnels. (art. 10(2)).
- La sensibilité des renseignements personnels est ajoutée comme facteur afin de déterminer la période de conservation. (art. 52(2)).

Aux articles 7 à 11, la LPVPC codifie et développe le principe de responsabilité actuellement énoncé à l'annexe 1 de la LPRPDÉ. Bien que les changements apportés aux exigences actuelles semblent relativement limités, certains ajouts notables à la LPVPC amélioreront sans doute la clarté de ces exigences pour les entreprises.

À la différence de la Loi 64 du Québec, il convient de noter que la LPVPC est silencieuse quant à l'obligation de procéder à une évaluation des facteurs relatifs à la vie privée dans certaines circonstances et quant à l'exigence du « respect de la vie privée dès la conception », deux éléments importants dans le cadre du régime de protection des renseignements personnels adopté par le Québec.

Renseignements personnels qui « relèvent » d'une organisation

Comme dans le cas de la LPRPDÉ, la LPVPC continue de prévoir qu'une organisation est responsable des renseignements personnels qui relèvent d'elle (art. 7(1) de la LPVPC remplaçant le principe 4.1 de la LPRPDÉ). Toutefois, la LPVPC va plus loin en définissant la notion de « relève », en précisant que les renseignements personnels « relèvent de l'organisation qui décide de les recueillir et établit les fins pour lesquelles ils sont recueillis, utilisés ou communiqués » (art. 7(2) de la LPVPC). Tout comme la LPRPDÉ, la LPVPC réitère que les renseignements personnels relèvent de l'organisation même lorsqu'ils ont été transférés à un fournisseur de services ou lorsque le fournisseur de services les recueille, utilise, ou communique pour le compte de l'organisation (art. 7(2) de la LPVPC, remplaçant le principe 4.1.3 de la LPRPDÉ). Tout comme le RGPD, la LPVPC distingue les obligations applicables aux organisations dont relèvent les renseignements personnels (notion proche de celle de « responsable du traitement » en vertu du RGPD) et celles applicables aux prestataires de services, ces derniers n'étant pas soumis à la Partie I du projet de loi (qui porte sur les obligations des organisations), à l'exception de l'article 57 (mesures de sécurité) et de l'article 61 (avis au client en cas d'atteinte aux mesures de sécurité).

Rôle du responsable de la protection de la vie privée

La LPVPC fait également écho à l'exigence de la LPRPDÉ selon laquelle une organisation doit désigner une personne « chargée des questions relatives aux obligations qui lui incombent » en vertu de la LPVPC (l'art. 8 LPVPC, remplaçant le principe 4.1.1 LPRPDÉ) et fournir les coordonnées professionnelles de la personne désignée à toute personne qui en fait la demande (l'art. 8 LPVPC remplaçant le principe 4.1.2 LPRPDÉ). Contrairement à la Loi 64 du Québec, qui attribue par défaut ce rôle à « la personne ayant la plus haute autorité » au sein de l'organisation (par exemple, le PDG), la LPVPC ne précise pas qui, au sein de l'organisation, doit remplir ce rôle.

Programme de gestion de la protection des renseignements personnels

La LPVPC exigera de chaque organisation qu'elle mette en œuvre et tienne à jour un « programme de gestion de la protection des renseignements personnels » qui comprend (mais sans doute sans s'y limiter) les politiques, pratiques et procédures que l'organisation met en œuvre pour remplir ses obligations au titre de la LPVPC. L'objet de ces politiques est généralement le même qu'en vertu de la LPRPDÉ : elles doivent porter sur la protection des renseignements personnels, le traitement des demandes de renseignements et des plaintes, la formation du personnel sur les politiques et les procédures, et l'élaboration de matériel pour expliquer les politiques et les procédures (l'art. 9(1) de la LPVPC remplaçant le principe 4.1.4 de la LPRPDÉ). Notamment, la LPVPC introduit une nouvelle exigence selon laquelle une organisation, lorsqu'elle élabore son programme de gestion de la protection des renseignements personnels, doit tenir compte du volume et de la nature sensible des renseignements personnels dont elle a la charge (art. 9(2) LPVPC). Cette mesure vise probablement à codifier la position actuelle du Commissaire selon laquelle les politiques et les mesures de protection des organisations doivent être raisonnables compte tenu des types de renseignements qu'elles traitent.

La LPVPC exigera également qu'une organisation donne au Commissaire l'accès à ses politiques, pratiques et procédures sur demande (art. 10(1) LPVPC). Bien que la LPRPDÉ ne contienne pas d'exigence équivalente, les organisations ont généralement fourni de tels documents au Commissaire lorsque ce dernier leur en a fait la demande. Le changement important est que la LPVPC prévoit qu'après examen de ces politiques, pratiques et procédures, le Commissaire peut fournir des conseils ou recommander des mesures correctives à l'organisation (art. 10(2) LPVPC).

Contrairement à la Loi 64 du Québec, qui oblige une organisation à publier de l'information détaillée sur ses politiques et procédures internes sur son site Web ou, si l'organisation n'a pas de site Web, par tout autre moyen approprié, la LPVPC ne semble pas imposer une exigence similaire en ce qui concerne son programme de gestion des renseignements personnels.

Consignation des fins

L'article 12(3) de la LPVPC exiger en outre qu'une organisation établisse et consigne chacune des fins pour lesquelles elle recueille, utilise ou communique des renseignements personnels, et qu'elle le fasse au moment de la collecte ou avant. À cet égard, la LPVPC semble aller plus loin que la LPRPDÉ (et que la Loi 64 du Québec), qui exige que les organisations documentent uniquement les fins de la collecte (principe 4.2.1 de la LPRPDÉ). Si elle établit que les renseignements personnels qu'elle a recueillis seront utilisés ou communiqués à une fin nouvelle, l'organisation doit consigner ladite fin avant d'utiliser ou de communiquer les renseignements personnels (art. 12(4) LPVPC).

Consentement

Consentement – Résumé des changements de C-27 par rapport à C-11 (2020)

- Les renseignements devant être fournis pour obtenir le consentement doivent l'être dans un langage clair et raisonnablement compréhensible pour l'individu. (art. 15(4)).
- Transparence (politiques de vie privée externes) : Des détails supplémentaires doivent être inclus dans les renseignements facilement accessibles sur les politiques et pratiques en matière de protection des renseignements personnels: (i) description des activités dans lesquelles l'organisation a un intérêt légitime et (ii) les périodes de conservation pour les renseignements de nature sensible. (art. 62(2)(b) et (e)).
- **Changement important** → Exception au consentement pour les « activités d'affaires »: Une organisation ne peut pas présumer le consentement implicite pour recueillir ou utiliser des renseignements dans le contexte d'une « activité d'affaires » – elles ne peuvent que se fier sur un consentement exprès ou satisfaire les critères prévus par l'exception des « activités d'affaires » (art. 15(6)). Les « activités d'affaires » n'incluent plus les activités menées à des fins de diligence raisonnable pour réduire ou prévenir les risques commerciaux de l'organisation (art. 18(2)(b)) et des « activités d'affaires » additionnelles peuvent être créées par règlement (art. 18(2)(d)). Nouvelle exception au consentement lorsque l'organisation a un intérêt légitime avec conditions associées, incluant l'obligation d'effectuer et de consigner une évaluation des intérêts légitimes (art. 18(3), (4) et (5)).
- Exception au consentement pour la prévention, détection et suppression de la fraude: L'exception s'applique également à l'utilisation des renseignements (plutôt qu'uniquement la collecte) (art. 27(2)).
- **Changement important** → L'exigence d'utiliser des renseignements dépersonnalisés au stade de la transaction commerciale éventuelle ne s'applique pas si cela nuit aux objectifs de l'éventuelle transaction et que l'organisation a tenu compte du risque de préjudice pour l'individu que pourrait entraîner l'utilisation ou la communication. (art. 22(2)).

Le projet de loi C-27 apporte des modifications importantes à la notion de consentement en introduisant une exception au consentement pour des activités d'affaires spécifiques - initialement proposée dans le cadre du C-11 (2020) - ainsi qu'une exception plus souple pour certains traitements effectués aux fins d'une activité dans laquelle l'organisation a un « intérêt légitime ». En outre, le projet de loi C-27 met en œuvre certaines recommandations clés formulées par le Commissaire dans son mémoire sur le projet de loi C-11 (2020), notamment en clarifiant la nécessité de normes objectives pour l'obtention d'un consentement valide et en exigeant une plus grande responsabilisation des organisations qui souhaitent se prévaloir d'exceptions plus larges en matière de consentement. Ce faisant, la LPVPC s'éloigne du modèle fortement critiqué, centré sur le consentement et favorisé par le régime législatif fédéral actuel, pour adopter une approche plus équilibrée qui reconnaît que le consentement n'est ni réaliste ni raisonnable dans toutes les circonstances. En bref, la LPVPC vise à établir un meilleur équilibre entre les intérêts commerciaux légitimes des organisations dans le traitement des renseignements personnels et le droit à la vie privée des Canadiens.

Le texte qui suit résume certaines des principales dispositions de la LPVPC relatives à la notion de consentement et à ses exceptions, tout en soulignant les modifications de fond apportées par la LPVPC par rapport à la LPRPDÉ et au projet de loi C-11 (2020).

Forme de consentement

Le consentement explicite demeure la forme de consentement par défaut en vertu de la LPVPC, mais une organisation peut se fonder sur le consentement implicite si cela est « approprié » dans les circonstances, compte tenu des « attentes raisonnables de l'individu » et de la « sensibilité » des renseignements personnels, aucune de ces deux notions n'étant toutefois définie explicitement dans la loi (art. 15(5)). Malgré l'absence d'une définition claire du terme « renseignements personnels sensibles », les renseignements personnels des « mineurs » - une notion qui est généralement définie par les lois de chaque province - sont expressément qualifiés par la loi de renseignements sensibles (art. 2(2) de la LPVPC), ce qui, à son tour, accroit la norme de consentement (entre autres exigences) pour ce type particulier de renseignements.

Pour les autres types de renseignements, la sensibilité devra être évaluée en fonction du contexte (voir le bulletin d'interprétation sur les renseignements sensibles du commissaire fédéral à la protection de la vie privée). Il est également intéressant de noter que le gouvernement fédéral n'a pas suivi l'approche du Québec qui, dans le cadre de sa réforme de la protection de la vie privée, a choisi de définir le terme « renseignements sensibles » comme des renseignements qui, en raison de leur nature, y compris les renseignements médicaux, biométriques ou autrement intimes, ou du contexte de leur utilisation ou de leur communication, comportent un niveau élevé d'attente raisonnable en matière de protection de la vie privée (art. 12 al. 4 (2) Loi 64).

Contrairement au projet de loi C-11 (2020), la LPVPC introduit une limite potentiellement importante à la notion de consentement implicite lorsque le traitement est effectué conformément à l'une des nouvelles exceptions au consentement pour des activités d'affaires déterminées ou légitimes en vertu de l'article 18 de la LPVPC. En particulier, l'article 15(6) de la LPVPC semble créer une règle selon laquelle le consentement implicite est jugé inapproprié si la collecte ou l'utilisation de renseignements personnels est effectuée pour une activité relevant de la nouvelle exception au consentement pour des activités d'affaires déterminées (art. 18(2)) ou pour des activités dans lesquelles l'organisation a un intérêt légitime (art. 18(3)).

L'intention semble être de renforcer la notion de consentement en exigeant des organisations qu'elles se fondent sur l'une des exceptions au consentement mentionnées ci-dessus ou qu'elles obtiennent un consentement explicite pour une ou plusieurs des activités décrites dans ces dispositions. Toutefois, compte tenu de l'ampleur des activités potentiellement couvertes par l'exception relative à l'intérêt légitime, il n'est pas clair dans quelle mesure une organisation peut s'appuyer sur le consentement implicite sans procéder au préalable à une évaluation de l'intérêt légitime conformément à l'article 18(4) de la LPVPC (comme indiqué plus en détail ci-dessous). Nous pouvons nous attendre à ce que la portée et l'application de l'article 15(6) de la LPVPC soient clarifiées à mesure que le projet de loi C-27 progresse dans le processus législatif.

Politique de vie privée et consentement éclairé

Quelle que soit la forme du consentement, une organisation doit fournir à la personne dont le consentement est sollicité certains types d'informations pour s'assurer que son consentement soit suffisamment éclairé. S'inspirant des Lignes directrices pour l'obtention d'un consentement valable du commissaire fédéral à la protection de la vie privée, l'article 15(3) de la LPVPC exige que les éléments suivants soient fournis avant ou au moment où le consentement est demandé:

- Fins auxquelles les renseignements personnels sont traités;
- Manière dont les renseignements personnels sont traités;
- Conséquence raisonnablement prévisible résultant des opérations de traitement.;
- Type précis de renseignements personnels qui doivent être traités; et
- Nom des tiers ou les catégories de tiers auxquels les renseignements personnels pourraient être communiqués.

Conformément au mémoire du Commissaire sur le projet de loi C-11 (2020), l'article 15(4) de la LPVPC précise maintenant que les renseignements décrits ci-dessus doivent non seulement être fournis en langage clair, mais aussi dans un langage suffisamment adapté au public cible pour qu'il soit raisonnable de s'attendre à ce qu'il soit « compréhensible » pour un individu visé par le contenu de l'avis. Cela correspond essentiellement à l'exigence énoncée à l'article 6.1 de la LPRPDÉ.

L'un des principaux problèmes que le projet de loi C-27 ne résout pas est la manière et le format dans lesquels cet avis doit être présenté à un individu. Par exemple, les outils généralement utilisés par les organisations pour présenter le contenu d'une manière plus pratique et plus accessible, tels que les avis en couches et les avis juste à temps, ne sont pas explicitement mentionnés, malgré la critique du Commissaire selon laquelle « une information en langage simple qui est difficile à trouver ou présentée dans un format qui rend la compréhension difficile ne mène pas à la compréhension (ou à un consentement valable) ». Malgré l'absence de règles claires sur le format, la structure du contenu et l'accessibilité de l'information, les organisations doivent néanmoins tenir compte des défis potentiels résultant du contexte global dans lequel le consentement est demandé lorsqu'elles déterminent comment fournir ou diriger activement les personnes vers les informations pertinentes.

Retrait du consentement et autres exigences clés

La LPVPC maintient en grande partie le *status quo* en ce qui concerne certaines des autres exigences clés de la LPRPDÉ en matière de consentement. Par exemple, le consentement aux opérations de traitement qui ne sont pas nécessaires à la fourniture d'un produit ou d'un service ne peut être une condition de service (**caractère facultatif du consentement**); une personne a le droit de retirer son consentement à tout moment, sous réserve d'un préavis raisonnable et des lois applicables ou des conditions raisonnables d'un contrat (**retrait du consentement**); et le consentement demeure invalide s'il a été obtenu en fournissant des renseignements faux ou trompeurs ou en utilisant des pratiques trompeuses ou mensongères (**consentement obtenu par subterfuge**).

Nouvelles exceptions au consentement

La plupart des exceptions relatives au consentement prévues par la LPRPDÉ sont répliquées dans la LPVPC avec des changements limités, le cas échéant. On mentionnera par exemple l'exception relative aux relations de travail (l'art. 24 de la LPVPC remplace l'art. 7.3 de la LPRPDÉ), aux renseignements sur le produit du travail (l'art. 23 de la LPVPC remplace l'art. 7(1)(b.2) de la LPRPDÉ) et aux transactions commerciales (l'art. 22 de la LPVCP remplace l'art. 7.2 de la LPRPDÉ).

Le LPVPC introduit également un certain nombre de nouvelles exceptions au consentement, notamment pour certaines activités d'affaires spécifiques. Par rapport au projet de loi C-11 (2020), cependant, la portée de l'exception pour les activités d'affaires spécifiques a été réduite, mais une nouvelle exception au consentement, plus souple, a été introduite pour les activités dans lesquelles une organisation a un intérêt légitime qui « l'emporte sur tout effet négatif potentiel sur l'individu » résultant de la collecte ou de l'utilisation de ses renseignements personnels. Ces exceptions, ainsi que quelques autres introduites spécifiquement pour les dépersonnalisées, sont examinées plus en détail ci-dessous.

Exception relative aux activités d'affaires spécifiques. Une organisation peut recueillir ou utiliser des renseignements personnels à l'insu de l'intéressé et sans son consentement si ce traitement est effectué aux fins d'une activité commerciale déterminée, autre que celle d'influencer le comportement ou les décisions de l'intéressé, et s'inscrit dans le cadre des attentes raisonnables de ce dernier (art. 18(1) de la LPVPC). En particulier, la LPVPC précise que les activités suivantes sont considérées comme des « activités d'affaires » :

- La fourniture d'un produit ou d'un service que l'individu a demandé à l'organisation;
- La sécurité des informations, des systèmes ou des réseaux de l'organisation;
- La sécurité d'un produit ou d'un service que l'organisation fournit; ou
- Toute autre activité réglementaire.

Toutefois, contrairement au projet de loi C-11 (2020), la notion d'« activité d'affaire » en vertu du projet de la LPVPC n'inclut plus une activité « exercée dans le cadre d'une diligence raisonnable visant à prévenir ou à réduire les risques commerciaux de l'organisation » ou « au cours de laquelle il serait impossible d'obtenir le consentement de la personne parce que l'organisation n'a pas de relation directe avec elle ». Ces exceptions semblent avoir été supprimées en réponse aux critiques de diverses parties prenantes qui estimaient que leur portée était trop large ou injustifiée.

Exception pour intérêt légitime. Un développement important est l'ajout d'une nouvelle exception souple d'intérêt légitime pour la collecte ou l'utilisation de renseignements personnels à l'insu de l'intéressé ou sans son consentement. En particulier, une organisation peut se prévaloir de cette exception lorsque les renseignements personnels sont recueillis ou utilisés aux fins d'une activité dans laquelle l'organisation a (i) un intérêt légitime qui l'emporte sur tout effet négatif potentiel sur l'individu résultant du traitement et (ii) qui n'implique pas d'influencer le comportement ou les décisions de l'individu, et (iii) que ce traitement répond aux attentes raisonnables de l'individu (art. 18(3) de la LPVPC).

Conformément aux demandes des régulateurs visant à associer un plus grand pouvoir d'utilisation des renseignements personnels à une plus grande responsabilisation des organisations et à une surveillance

réglementaire, une organisation doit, avant de se prévaloir de cette exception, effectuer et consigner une évaluation de l'intérêt légitime et, sur demande, en fournir une copie au Commissaire. En particulier, l'évaluation de l'intérêt légitime doit :

- Identifier tout effet négatif potentiel résultant des opérations de traitement pertinentes;
- Identifier les mesures raisonnables mises en œuvre pour réduire la probabilité que les effets se produisent ou pour les atténuer ou les éliminer; et
- Démontrer la conformité à toute autre exigence prescrite par la réglementation.

Bien qu'une organisation qui se fonde sur cette exception puisse recueillir et utiliser des renseignements personnels à l'insu d'un individu et sans son consentement, il convient de noter qu'une organisation doit néanmoins faire preuve de transparence dans sa politique de protection de la vie privée quant à la façon dont elle applique les exceptions relatives au consentement, notamment en fournissant une description de toute activité relevant de l'exception relative à l'intérêt légitime (art. 62(2)(b) de la LPVPC).

D'autre part, bien que similaire à la notion d'intérêt légitime du RGPD, l'exception d'intérêt légitime de la LPVPC a probablement été modelée sur la *Personal Data Protection Act* (« **PDPA** ») de Singapour, dont l'exception équivalente reste également intégrée dans un cadre de consentement. En d'autres termes, l'exception d'intérêt légitime de la LPVPC n'est qu'une exception au consentement, et non une base juridique alternative et distincte pour le traitement des données sur un pied d'égalité avec le consentement. Toutefois, contrairement à la PDPA et au RGPD, cette exception ne s'applique pas à la divulgation de renseignements personnels à un tiers et ne permet pas explicitement de prendre en compte l'intérêt légitime d'une autre personne (c'est-à-dire autre que celui de l'organisation qui collecte ou utilise les informations). En tout état de cause, il n'est pas clair à ce stade quels types d'activités spécifiques pourraient ou non relever de l'« intérêt légitime » d'une organisation et, en particulier, si cela pourrait s'étendre à l'amélioration des produits, au développement de nouveaux produits ou services, voire à certaines formes de publicité ou de marketing, telles que le marketing direct ou la publicité basée sur la localisation.

Exceptions spécifiques pour les renseignements dépersonnalisés. En plus de permettre l'utilisation de renseignements personnels à l'insu de l'intéressé ou sans le consentement de l'individu pour les dépersonnaliser (art. 20), la LPVPC offre aux organisations les exceptions suivantes en matière de consentement pour les renseignements dépersonnalisés, qui sont, pour la plupart, conformes à ce qui avait été proposé précédemment dans le cadre du projet de loi C-11 (2020), à savoir :

- **Exception pour les fins socialement bénéfiques (art. 39 LPVPC).** Une organisation peut communiquer des renseignements dépersonnalisés à une institution gouvernementale ou à d'autres tiers désignés si cette divulgation est faite dans une « fin socialement bénéfique », qui concerne la santé, la fourniture ou l'amélioration d'équipements ou d'infrastructures publics, la protection de l'environnement ou tout autre but déterminé par la réglementation.
- **Exception pour la recherche, l'analyse et le développement (art. 21 LPVPC).** Une organisation peut utiliser des renseignements dépersonnalisés à des fins de recherche, d'analyse et de développement internes.

Bien que la LPVPC continue d'exiger des parties à une transaction commerciale éventuelle qu'elles dépersonnalisent les renseignements personnels (en plus d'autres exigences) afin de pouvoir utiliser ou communiquer ces renseignements à l'insu de l'intéressé et sans son consentement (art. 22(1)), cette exigence a été tempérée. En particulier, l'organisation n'est pas tenue de dépersonnaliser les renseignements avant de les utiliser ou de les communiquer si ceci compromet les objectifs de la transaction et si l'organisation a tenu compte du risque de préjudice résultant d'un tel traitement (art. 22(2)).

Évaluation du caractère raisonnable (fins acceptables)

Évaluation du caractère raisonnable (fins acceptables) – Résumé des changements de C-27 par rapport à C-11 (2020)

- Codification de la jurisprudence prévoyant qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins et d'une manière qu'une personne raisonnable estimerait acceptable dans les circonstances, *que le consentement soit requis ou non* (art. 12(1)).

La LPRPDÉ comprend une évaluation du caractère raisonnable (c'est-à-dire le test de la « personne raisonnable »), qui dicte les limites de son application et qui peut s'appliquer même si le consentement a été obtenu. La LPVPC comprend cette même exigence selon laquelle une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins et d'une manière qu'une personne raisonnable estimerait acceptables dans les circonstances (l'art. 12(1) de la LPVPC remplaçant l'art. 5(3) de la LPRPDÉ). Bien que cette disposition de la LPVPC sous C-27 soit semblable à celle prévue par la LPRPDÉ et par le projet de loi C-11 (2020), l'expression « et d'une manière » a été ajoutée dans le projet de loi C-27 ; le texte précise également que ce critère de caractère raisonnable s'applique « que le consentement soit requis ou non aux termes de la présente loi ».

La LPVPC prévoit les facteurs qui doivent être pris en compte pour déterminer le caractère acceptable des fins et de la manière de recueillir, utiliser ou communiquer des renseignements personnels. Ces facteurs sont en grande partie les mêmes que ceux élaborés dans la décision *Turner* c. *Telus Communications Inc*. de la Cour fédérale – décision ultérieurement confirmée par la Cour d'appel fédérale –, dans laquelle furent énoncés les facteurs permettant d'évaluer si les fins d'une organisation étaient conformes à l'article 5(3) LPRPDÉ. Ces facteurs sont les suivants :

- la mesure dans laquelle les renseignements personnels sont de nature sensible;
- le fait que les fins visées correspondent à des besoins commerciaux légitimes de l'organisation
- le degré d'efficacité de la collecte, de l'utilisation ou de la communication pour répondre aux besoins commerciaux légitimes de l'organisation;
- l'existence ou non de moyens portant une atteinte moindre à la vie privée de l'individu et permettant d'atteindre les fins visées à un coût et avec des avantages comparables;
- la proportionnalité entre l'atteinte à la vie privée de l'individu et les avantages pour l'organisation, au regard des moyens, techniques ou autres, mis en place par l'organisation afin d'atténuer les effets de l'atteinte pour l'individu (art. 12(2) LPVPC).

Comme le libellé de la nouvelle disposition est similaire à celui utilisé dans la LPRPDÉ, le Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3), publié par la Commissaire en mai 2018, demeure pertinent.

Tel que discuté ci-dessus (voir « Consignation des fins » dans la section relative à la Responsabilité), en vertu de la LPVPC, l'organisation doit établir et consigner les fins auxquelles les renseignements personnels sont recueillis, utilisés ou communiqués avant la collecte ou au plus tard au moment de celle-ci (art. 12(3) et (4) LPVPC).

Alors que les amendements récents du Québec ne comprennent pas un test d'évaluation du caractère raisonnable similaire, dans l'analyse de la nécessité de la collecte de renseignements personnels, il est à noter qu'en vertu de l'article 5 de la Loi sur le secteur privé du Québec, la CAI évalue si l'objectif poursuivi est important, légitime et réel, ainsi que la proportionnalité entre l'objectif poursuivi et l'atteinte à la vie privée que constitue cette collecte (*Institut généalogique Drouin Inc.*, CAI 091570, décision de D. Poitras, 6 février 2015.)

Droits individuels

Droits individuels – Résumé des changements de C-27 par rapport à C-11 (2020)

- **Changement important** ➔ Les droits individuels ne s'appliquent pas aux renseignements dépersonnalisés (art. 2(3)).
- **Changement important** ➔ Système décisionnel automatisé : l'obligation de fournir une explication relativement à un système décisionnel automatisé ne s'applique qu'à la prédiction, recommandation ou décision qui pourrait avoir une incidence importante pour l'individu. (art. 63(3)).
- **Changement important** ➔ Droit de retrait : nouvelles conditions (art. 55(1) et nouvelles exceptions (55(2)).

De façon similaire à la LPRPDÉ, la LPVPC accordera aux individus le droit d'accéder à leurs renseignements personnels et de les corriger (accès et rectification). La LPVPC accorde également aux individus de nouveaux droits quant aux systèmes décisionnels automatisés, un droit de supprimer (retrait) des renseignements personnels et un droit de les faire transférer d'une organisation à l'autre dans des circonstances limitées. Point à noter, la LPVPC exclue expressément les renseignements personnels qui ont été dépersonnalisés de certaines dispositions relatives aux droits individuels.

Droit d'accès et de rectification

Les articles 63 à 71 de la LPVPC détaillent les droits d'accès et de rectification des renseignements personnels. Sous réserve des exceptions limitées précisées ci-dessous, les dispositions concernant les droits d'accès et de rectifications de la LPVPC ne s'écartent pas du précédent régime de la LPRPDÉ (articles 8 et 9 et principe 4.9).

Information concernant la conservation, l'utilisation et la communication aux tiers. De la même façon que sous la LPRPDÉ, après réception d'une demande écrite d'un individu, une organisation sera tenue de lui indiquer en langage clair : si elle détient des renseignements personnels à son sujet, comment elle utilise les renseignements personnels et si l'organisation a communiqué ses renseignements; et, lorsqu'elle a communiqué ses renseignements, de lui fournir le nom des tiers ou des types de tiers auxquels la communication a été faite (y compris lorsque cette communication a été faite sans l'obtention du consentement). Concernant cette dernière exigence, la LPRPDÉ permet à une organisation, lorsqu'il n'est pas possible de fournir une liste précise des tiers, de fournir une liste des organisations auxquelles elle *peut* avoir communiqué ces renseignements personnels – une option qui semble avoir été omise dans la LPVPC (art. 63(1) et (2) de la LPVPC remplaçant le principe 4.9.3 de la LPRPDÉ).

Amendement et consignation du désaccord. Comme dans la LPRPDÉ, si une organisation octroie à un individu l'accès à ses renseignements personnels, et si celui-ci démontre que ses renseignements personnels sont inexacts, désuets ou incomplets, la LPVPC impose à l'organisation de rectifier ses renseignements et d'informer tout tiers qui y a accès de la rectification. Si l'organisation est en désaccord avec l'individu au sujet des rectifications demandées, elle doit consigner ce désaccord et en informer les tiers (art. 71 et 71(3) de la LPVPC remplaçant les principes 4.9.5 et 4.9.6 de la LPRPDÉ).

Conservation des renseignements utilisés pour prendre une décision. Comme le prévoit la LPRPDÉ, la LPVPC exige que l'organisation qui utilise des renseignements personnels pour prendre une décision à propos d'un individu de conserver les renseignements pendant une période suffisante pour permettre à l'individu de faire une demande d'accès ou de rectification de ses renseignements personnels (art. 54 LPVPC remplaçant le principe 4.5.2 de la LPRPDÉ). Une organisation qui détient des renseignements personnels au sujet d'un individu ayant fait une requête pour savoir si l'organisation détient des renseignements personnels, les utilise et les communique, doit conserver les renseignements le temps nécessaire pour permettre à l'individu d'épuiser tous les recours disponibles dans la LPVPC (art. 69 LPVPC remplaçant l'art. 8(8) LPRPDÉ). La LPVPC fixe cette période de conservation à six mois à compter de la date du refus d'acquiescer à la demande (ou du défaut de répondre à cette demande), mais le Commissaire peut décider de prolonger ce délai (art. 54 et 82(3) de la LPVPC).

Droit d'être informé des systèmes décisionnels automatisés

La LPVPC accorde aux individus un nouveau droit de recevoir une explication sur l'utilisation de système décisionnel automatisé pour faire une prédiction, une recommandation ou pour prendre une décision à leur sujet qui pourrait avoir une incidence importante sur eux – un droit individuel également présent à la fois dans la Loi 64 du Québec et le RGPD mais non dans la LPRPDÉ (art. 63(3) de la LPVPC). Contrairement à la Loi 64 du Québec et au RGPD, les dispositions relatives au système décisionnel automatisé de la LPVPC n'accordent pas aux individus le droit de s'opposer à une telle utilisation ou de faire réviser la décision par un employé de l'organisation (pour plus d'information sur les dispositions de la LPVPC concernant les systèmes décisionnels automatisés, voir la section intitulée « Dépersonnalisation, recherche et analyse de données » ci-dessous).

Droit au retrait

L'article 55 de la LPVPC établira un nouveau droit pour les individus de demander le retrait de leurs renseignements personnels (c'est-à-dire leur suppression permanente et irréversible) par une organisation de qui relèvent ces renseignements sous certaines conditions, soit si : (a) l'organisation a recueilli, utilisé ou communiqué les renseignements personnels en contravention de la LPVPC ; (b) l'individu a retiré son consentement à la collecte, l'utilisation ou la communication des renseignements personnels ; ou (c) les renseignements personnels ne sont plus nécessaires à la fourniture continue du bien ou du service à l'individu.

La LPVPC permet à une organisation de refuser une telle demande de retrait sous certaines conditions, si (i) le retrait entrainerait également celui de renseignement personnel d'un autre individu qui ne peuvent être retranchés, (ii) un engagement contractuel ou une loi empêche de procéder au retrait, (iii) le retrait aurait un effet négatif excessif sur l'intégrité ou l'exactitude des renseignements nécessaires à la fourniture continue d'un produit ou d'un service, (iv) la demande de l'individu est vexatoire ou entachée de mauvaise foi – ou de façon plus importante – (v) le retrait des renseignements est déjà prévu conformément aux politiques de conservation de l'organisation et celle-ci informe l'individu de la période de conservation restante qui est applicable à ces renseignements. Plusieurs de ces conditions permettant à une organisation de refuser une telle demande de retrait n'étaient pas présentes sous C-11 (2020) et ont été introduites sous C-27.

Il est intéressant de noter que ce droit de retrait ne semble pas englober un droit de désindexation ou un droit à l'oubli, contrairement à la Loi 64 du Québec et au RGPD.

Droit à la mobilité des renseignements personnels

La LPVPC innove à l'article 72 en créant un droit limité à la portabilité des données, qui permettra aux individus de demander à une organisation que leurs renseignements personnels soient communiqués à une autre organisation, qu'ils désignent, dans la mesure où les deux organisations soient soumises à un « cadre de mobilité des données » (qui sera déterminé par règlements selon la LPVPC). Il est important de noter que ce droit s'appliquera uniquement aux renseignements personnels recueillis auprès des individus (et non pas auprès de tiers). La LPVPC indique que des règlements peuvent établir les garanties pour la divulgation sécurisée des renseignements et des paramètres pour les moyens techniques permettant d'assurer l'interopérabilité (art. 123). Les règlements pourront aussi préciser les organisations soumises au cadre, ce qui semble suggérer que le droit à la mobilité des renseignements personnels de la LPVPC pourrait être limité à certains secteurs industriels spécifiques (tels que les banques ou les télécommunications). À noter, le droit à la mobilité des renseignements personnels sera plus limité que celui de la Loi 64 du Québec et du RGDP en raison des restrictions relatives aux organisations qui peuvent faire l'objet d'une telle demande de portabilité des données. Par conséquent, la LPVPC n'ouvre pas complètement la porte à des demandes générales de portabilité telles que prévues dans la Loi 64 du Québec et le RGPD.

Avertissement : renseignement dépersonnalisé et droits des individus

Fait intéressant, la LPVPC introduit une nouvelle exception à certains droits individuels. La LPVPC prévoit que les renseignements qui ont été dépersonnalisés *ne seront pas* considérés comme des renseignements personnels aux fins du droit de retrait, du droit d'accès et de rectification ainsi qu'au droit à la mobilité des renseignements. Le droit d'être informé des systèmes décisionnels automatisés continue cependant de s'appliquer aux renseignements dépersonnalisés (art. 2(3) de la LPVPC)).

Dépersonnalisation, recherche et analyse de données

Dépersonnalisation, recherche et analyse de données – Résumé des changements de C-27 par rapport à C-11 (2020)

- **Changement important** → Définition révisée de « dépersonnaliser » : Modifier des renseignements personnels afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement » (art. 2).
- **Changement important** → Nouvelle définition d'« anonymiser » : « Modifier définitivement et irréversiblement, conformément aux meilleures pratiques généralement reconnues, des renseignements personnels afin qu'ils ne permettent pas d'identifier un individu, directement ou indirectement, par quelque moyen que ce soit » (art. 2).
- **Changement important** → Reconnaissance explicite que la LPVPC ne s'applique pas aux renseignements ayant été anonymisés. [art. 6(5)] et exceptions additionnelles à l'interdiction de ré-identifier des renseignements ayant été dépersonnalisés (art. 75).
- Sur demande de l'organisation, le Commissaire peut l'autoriser à ré-identifier un individu en utilisant des renseignements dépersonnalisés lorsqu'il l'estime manifestement dans l'intérêt de l'individu (art. 116).
- L'exception au consentement pour l'utilisation de renseignements dépersonnalisés à des fins de recherche et de développement s'étend aussi à l'analyse (art. 21).
- **Changement important** → L'exception au consentement permettant la communication de renseignements personnels n'est plus limitée aux fins d'étude ou de recherche érudites (art. 35)

La LPVPC introduit une définition de renseignements « anonymisés » et « dépersonnalisés » ainsi que certaines circonstances dans lesquelles les renseignements dépersonnalisés ne seront pas considérés comme des renseignements personnels. Ces changements permettront aux organisations de bénéficier d'une plus grande flexibilité quant au traitement de renseignements dépersonnalisés, incluant pour des fins de recherches internes et d'analyse de données.

Dépersonnalisation et anonymisation

La LPVPC introduit une distinction claire entre des renseignements dépersonnalisés et des renseignements anonymisés, contrairement au projet de loi antérieur C-11 (2020). En vertu de la LPVPC, « dépersonnaliser » signifie « modifier des renseignements personnels afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement » (art. 2). « Anonymiser » signifie plutôt « modifier définitivement et irréversiblement, conformément aux meilleures pratiques généralement reconnues, des renseignements personnels afin qu'ils ne permettent pas d'identifier un individu, directement ou indirectement, par quelque moyen que ce soit. » (art. 2). À cet égard, l'approche de la LPVPC est alignée avec la Loi 64 du Québec,

qui introduit des distinctions similaires. Bien qu'il y ait certaines différences avec les définitions qui entreront prochainement en vigueur au Québec, il se dégage de ces nouvelles dispositions une harmonisation des approches des différents commissaires à la vie privée canadiens. Par exemple, les deux textes prévoient pour la dépersonnalisation l'élimination des identifiants directs et pour l'anonymisation la modification irréversible de renseignements personnels pour des renseignements qui ne permettent plus d'identifier un individu, directement ou indirectement.

De manière importante, la LPVPC établit que la dépersonnalisation d'un renseignement personnel est une utilisation qui ne requiert pas la connaissance ou le consentement des individus (art. 20). La LPVPC prévoit également que l'anonymisation est considérée comme une forme de retrait (art. 2(1)), et les organisations ont toujours une obligation de retirer les renseignements personnels qui ne sont plus nécessaires pour réaliser les fins auxquelles ils ont été recueillis, utilisés ou communiqués ou pour se conformer aux lois applicables (s. 53(1)). Conséquemment, la LPVPC prévoit un cadre réglementaire qui permet aux organisations de dépersonnaliser ou anonymiser des renseignements personnels sans la nécessité d'obtenir un consentement spécifique à ces fins, mettant fin à une ambiguïté présente sous la LPRPDÉ.

Le seuil relativement faible pour la dépersonnalisation – retrait d'identifiants directs – permettra aux organisations de préserver la richesse des données d'archivage essentielles pour la recherche interne. Cependant, la LPVPC prévoit certaines mesures à respecter et certaines restrictions concernant le traitement de renseignements personnels dépersonnalisés. L'article 74 prévoit en effet qu'une organisation qui dépersonnalise des renseignements personnels doit s'assurer que tous les procédés techniques et administratifs utilisés soient proportionnels aux fins auxquelles ces renseignements sont dépersonnalisés et à la nature sensible des renseignements personnels. L'article 75 prohibe l'utilisation des renseignements personnels qui ont été dépersonnalisés, seuls ou en combinaison avec d'autres renseignements, afin d'identifier un individu, sauf : (a) pour vérifier l'efficacité des mesures de sécurité mises en place; (b) pour se conformer aux exigences prévues sous le régime de la LPVPC ou à celles du droit fédéral ou provincial; (c) pour vérifier l'équité et l'exactitude des modèles, des processus et des systèmes élaborés à l'aide des renseignements dépersonnalisés; (d) pour vérifier l'efficacité de ses processus de dépersonnalisation; (e) ou dans tout autre cas prévu ou autorisé. Par ailleurs, les organisations qui contreviennent sciemment à l'article 75 sont passibles d'une amende pouvant atteindre 25 000 000 $ ou 5 % de leurs recettes globales brutes, selon le plus élevé des deux montants (art. 128 (a)). Ces dispositions reconnaissent implicitement le risque inhérent à la ré-identification associée à certaines formes de dépersonnalisation, et visent à équilibrer l'utilisation de ces renseignements et les protections/restrictions qui devraient être mises en place pour minimiser un tel risque.

Un changement important de l'ancienne version de la LPVPC est l'introduction de circonstances pour lesquels des renseignements dépersonnalisés ne sont pas considérés comme des renseignements personnels. L'article 2(3) de la LPVPC dispose que : « [p]our l'application de la présente loi, à l'exception des articles 20 et 21, des paragraphes 22(1) et 39(1), des articles 55 et 56, du paragraphe 63(1) et des articles 71, 72, 74, 75 et 116, les renseignements personnels qui ont été dépersonnalisés sont considérés comme étant des renseignements personnels » (nos soulignements). L'examen de ces exceptions révèle un cadre soigneusement étudié qui répond aux défis que soulève le traitement de renseignements personnels dépersonnalisés lorsqu'ils sont traités de la même manière que des renseignements personnels standards. Par exemple, les obligations des organisations de procéder au retrait des renseignements personnels sur demande de l'individu (art. 55), de maintenir l'exactitude des renseignements (art. 56), de donner accès ou

d'amender sur demande (art. 63(1) et 71(1)) sont toutes inapplicables aux renseignements dépersonnalisés. Collectivement, ces articles motiveront les organisations à dépersonnaliser les renseignements personnels avant de les utiliser pour des fins de recherche et de développement (plutôt que d'obtenir le consentement et d'utiliser les renseignements personnels dans leur forme originale) en rendant inapplicables plusieurs obligations qui rendraient la dépersonnalisation difficile en pratique.

Finalement, nous notons que la LPVPC ne s'applique pas à des renseignements personnels qui ont été anonymisés (art. 2(5)).

Recherche

La LPVPC introduira une nouvelle exception au consentement qui permettra aux organisations d'utiliser de renseignements personnels à des fins de recherche et de développement internes si les renseignements sont dépersonnalisés avant d'être utilisés (art. 21). De façon semblable à la Loi 64 du Québec, la LPVPC permettra ainsi aux organisations de réutiliser les renseignements personnels recueillis pour des fins spécifiques pour des fins de recherche secondaire, comme l'analytique d'entreprise ou d'affaires. Les amendements apportés à l'article 75 confirment aussi ce qui était attendu concernant l'utilisation de renseignements dépersonnalisés pour l'apprentissage automatique (« *machine learning* »), à savoir qu'ils seront aussi couverts par la « recherche et développement » prévu par cette exception.

Systèmes décisionnels automatisés et intelligence artificielle

Nous abordons dans cette section les dispositions gouvernant les systèmes décisionnels automatisés dans le contexte de la LPVPC, à la fois telles qu'exposées au sein de la LPVPC et dans le contexte des interactions potentielles avec certaines dispositions de la nouvelle *Loi sur l'intelligence artificielle et les données* (« LIAD »). Nous aborderons en détail la LIAD dans un bulletin distinct.

Nous notons de prime abord que les termes centraux de la LPVPC et de la LIAD se chevauchent, sans être identiques. La LPVPC définit « système décisionnel automatisé » comme une « technologie utilisant des systèmes basés sur des règles, l'analyse de régression, l'analytique prédictive, l'apprentissage automatique, l'apprentissage profond, des réseaux neuronaux ou d'autres techniques afin d'appuyer ou de remplacer le jugement de décideurs humains » (art. 2 LPVPC). La LIAD aborde la notion de « système d'intelligence artificielle », définit comme un « système technologique qui, de manière autonome ou partiellement autonome, traite des données liées à l'activité humaine par l'utilisation d'algorithmes génétiques, de réseaux neuronaux, d'apprentissage automatique ou d'autres techniques pour générer du contenu, faire des prédictions ou des recommandations ou prendre des décisions » (art. 2 LIAD). Ces différences de portée ne sont pas surprenantes, considérant que la LPVPC adresse l'exactitude des décisions rendues par des systèmes décisionnels automatisés qui utilisent des renseignements personnels, alors que la LIAD régit les risques plus généraux occasionnés par les systèmes d'intelligence artificielle aux droits des individus.

Nous retrouvons aussi certaines différences potentielles de juridiction entre les deux projets de loi, la LPVPC s'appliquant dans un cadre intra provinciale dans la mesure où il n'y a pas de loi provinciale déclarée par règlement comme essentiellement semblable (art. 122(3) de la LPVPC), tandis que la LIAD semble s'appliquer expressément aux activités exercées dans le cadre des échanges de commerce internationaux ou interprovinciaux (art. 5(1) LIAD).

Malgré les différences de portée et de juridiction, les deux lois risquent de se chevaucher et, dans certaines circonstances, les obligations de la LPVPC pourraient être remplacées par des obligations plus strictes prévues par la LIAD, tel que détaillé ci-dessous. En effet, la LPVPC aborde les systèmes décisionnels automatisés dans trois contextes : (i) « Ouverture et transparence » (art. 62 LPVPC), (ii) « Accès et rectification » (art. 63 à 71 LPVPC), et (iii) dans le contexte de restriction d'utilisation de renseignements dépersonnalisés (art. 75 LPVPC).

Ouverture et transparence

Conformément au principe d'ouverture et de transparence, une organisation qui utilise un système décisionnel automatisé doit rendre facilement accessible, dans un langage clair une explication générale de l'usage qu'elle fait de tels systèmes pour faire des prédictions, formuler des recommandations ou prendre des décisions qui pourraient avoir une incidence importante sur les individus concernés (art. 62(2)(c)). L'expression « incidence importante » n'est pas définie ou précisée. Cette notion pourrait inclure des circonstances susceptibles d'entraîner un « préjudice grave », telle que l'expression est définie à l'article 58(7) de la LPVPC, incluant des circonstances impliquant la réputation, l'emploi, les finances ou le crédit.

Les organisations devront porter attention aux précisions qui seront apportées au terme « système à incidence élevée » tel qu'utilisé au sein de la LIAD. Le critère pour la qualification de système à incidence élevée sera en effet établi par règlement (art. 5(1) LIAD). L'utilisation de systèmes à incidence élevée entraîne aussi des obligations de transparence, qui vont au-delà des exigences prévues par la LPVPC pour les systèmes décisionnels automatisés qui pourrait avoir une incidence importante. Plutôt que de fournir uniquement une explication générale, les utilisateurs de systèmes à incidence élevée devront publier en langage clair une description du système comprenant des explications sur l'utilisation qui en est faite, le contenu qu'il génère et les décisions, recommandations ou décisions qu'il prend, les mesures d'atténuation mise en place pour les risques de préjudice ou de résultats biaisés créés par le système, et tout autre renseignement prévu par règlement (art. 11(2) LIAD). Les organisations devront trouver un équilibre entre le respect des obligations de transparence et la protection de leurs renseignements d'affaires confidentiels (bien que la LIAD considère cet aspect et contient certaines dispositions à cet égard (art 5(1), 18(1), 22-29 LIAD) et de ceux qui permettraient à des tierces parties non autorisées d'utiliser ces systèmes.

Conséquemment, considérant les interactions évidentes entre les deux projets de loi, le législateur semble vouloir différencier « incidence importante » et « système à incidence élevée », avec de plus grandes obligations de transparence pour les systèmes à incidence élevée qui s'aligne aussi avec la définition de système décisionnel automatisé en vertu de la LPVPC.

Accès et rectification de renseignements personnels

Selon le principe d'accès et de rectification de renseignements personnels, si une organisation a utilisé un système décisionnel automatisé pour faire une prédiction, formuler une recommandation ou prendre une décision concernant un individu, l'organisation devra, à la demande de l'individu, lui fournir une explication de la prédiction, recommandation ou décision (art. 63(1)(3) LPVPC). L'explication doit indiquer le type de renseignements personnels utilisés pour faire la prédiction, formuler la recommandation ou prendre la décision, la provenance de ces renseignements ainsi que les motifs ou les principaux facteurs ayant mené à la prédiction, à la recommandation ou à la décision (art. 63(4) LPVPC). Ces articles de la LPVPC ont été amendés par rapport à l'ancien projet de loi C-11 (2020) et sont cohérents avec les articles de la Loi 64 du Québec.

Les clarifications apportées à l'obligation de fournir des explications sont plus utiles que les dispositions figurant dans la version antérieure, mais pourraient tout de même présenter un défi avec les exigences additionnelles de l'art. 66(1) de la LPVPC, qui requiert que les organisations fournissent l'information à l'individu dans un langage clair. Contrairement à l'exigence de « langage clair », prévu aux articles régissant les principes d'ouverture et de transparence, qui est satisfaite en fournissant une « explication générale », il n'est pas clair si un langage clair pour une prédiction, recommandation ou décision pouvait être fourni lorsque le système utilisé est fondé sur l'apprentissage automatique (*machine learning*), l'apprentissage profond (*deep learning*) ou des réseaux neuronaux (*neural network*).

La LPVPC ne prévoit pas de droit individuel additionnel autre que celui d'obtenir des explications. On soulignera que la Loi 64 au Québec prévoit que les individus peuvent soumettre leurs observations à une personne désignée au sein de l'entreprise qui peut réviser la décision. De plus, bien que l'article 71(1) permette aux individus d'apporter les modifications requises aux renseignements personnels les concernant s'ils démontrent à l'organisation que les renseignements sont désuets, inexacts ou incomplets, la LPVPC ne comprend pas de base juridique pour contester une décision prise par un système décisionnel automatisé.

Réidentification

La LPVPC introduit une exception intéressante à l'interdiction générale d'utiliser sciemment des renseignements personnels dépersonnalisés pour réidentifier un individu. L'article 75(c) de a LPVPC prévoit que des renseignements dépersonnalisés peuvent être utilisés pour identifier un individu pour « vérifier l'équité et l'exactitude des modèles, des processus et des systèmes élaborés à l'aide des renseignements dépersonnalisés ». Le terme « modèles » est probablement utilisé pour faire référence au résultat du processus d'apprentissage automatique (*machine learning*) conformément à la littérature consacrée à ce sujet. Avec cette interprétation, l'article 75(c) de la LPVPC va de concert avec l'obligation prévue dans la LIAD pour les personnes responsables des systèmes à incidence élevée d'identifier et de mettre en place des mesures d'atténuation pour les risques de préjudice ou de résultats biaisés.

L'évaluation (*testing*) de modèles d'apprentissage automatique (*machine learning*) utilisés pour des systèmes à incidence élevée présentant un risque de préjudice ou de résultat biaisés, ne sera pas affectée par le risque de réidentification dans la mesure où celui-ci existe parce que les données utilisées pour entrainer le modèle ont été dépersonnalisées. Par contre, il reste à voir si l'exception à l'interdiction générale de réidentification sera interprétée par les régulateurs comme impliquant que tous les modèles, processus et systèmes devraient être soumis à de telles évaluations, qu'ils soient définis ou non comme un système à incidence élevée par les règlements de la LIAD.

Impartition et transferts transfrontaliers

La LPVPC ne modifie pas de manière notable les exigences relatives à l'impartition ou aux transferts transfrontaliers. Elle intègre plutôt formellement les exigences et les meilleures pratiques existantes, et clarifie les rôles et les obligations de l'organisation dont relèvent les renseignements personnels et de ses fournisseurs de services. Pour les entreprises, ces changements seront probablement les bienvenus puisqu'ils apporteront plus de clarté et de cohérence.

Impartition

La LPVPC apporte des précisions opportunes en ce qui concerne le transfert de renseignements personnels à un fournisseur de services, que la LPVPC définit comme « toute organisation, notamment une société mère, une filiale, une société affiliée, un entrepreneur ou un sous-traitant, qui fournit un service au nom ou pour le compte d'une autre organisation pour lui permettre de réaliser ses fins » (art. 2).

L'article 19 de la LPVPC confirme que les organisations peuvent transférer les renseignements personnels d'un individu à un tiers fournisseur de services à l'insu de l'intéressé et sans requérir son consentement, ce qui mettra un terme définitif à plusieurs années tumultueuses au cours desquelles le Commissaire a adopté, puis renversé, sa position selon laquelle le transfert de renseignements personnels à des fins de traitement nécessitait un consentement explicite supplémentaire.

La LPVPC précise aussi les principes et exigences suivants qui seront applicables aux contrats d'impartition impliquant des renseignements personnels :

- La LPVPC prévoit que les renseignements personnels recueillis, utilisés ou divulgués au nom d'une organisation par un fournisseur de services relèvent de l'organisation (et non du fournisseur de services) si cette organisation décide de les recueillir et établit les fins de leur collecte, de leur utilisation ou de leur communication (art. 7(2)).
- Comme sous la LPRPDÉ, la LPVPC impose à une organisation qui transfère des renseignements personnels à un tiers fournisseur de services la responsabilité de veiller (contractuellement ou autrement) à ce que le fournisseur de services offre un niveau de protection équivalent à ce que l'organisation est tenue d'offrir pour ces renseignements personnels selon la LPVPC (art. 11(1)).
- La LPVPC précise que la plupart des obligations énoncées dans sa partie 1 ne s'appliquent pas à un fournisseur de services relativement aux renseignements personnels qui lui sont transférés par l'organisation aux fins de traitement. Cependant, un fournisseur de services sera sujet à toutes les obligations de la partie 1 de la LPVPC s'il recueille, utilise ou communique des renseignements personnels pour des fins autres que pour celles pour lesquelles les renseignements lui ont été transférés (art. 11(2)).
- La LPVPC confirme que les fournisseurs de services doivent protéger les renseignements personnels au moyen de mesures de sécurité matérielles, organisationnelles et techniques qui sont proportionnelles à la sensibilité de ces renseignements (art. 57).
- Si une organisation procède au retrait de renseignements personnels à la demande d'un individu, alors l'organisation doit, dès que possible, informer chaque fournisseur de services à qui l'organisation a transféré les renseignements et veiller à ce qu'il ait procédé à ce retrait (art. 55(4)); et

- Un fournisseur de services qui subit une atteinte aux mesures de sécurité doit, dès que possible, aviser l'organisation de qui relèvent ces renseignements personnels (art. 61; voir la section « Mesures de sécurité et réponse aux incidents » pour plus d'information).

Il convient également de mentionner, à titre comparatif, que la Loi 64 du Québec comporte des exigences similaires en matière d'impartition, bien que ses exigences relatives au contenu des contrats d'impartition soient plus prescriptives que celles de la LPVPC.

Transferts transfrontaliers et coopération

L'article 6(2) de la LPVPC confirme que la LPVPC s'applique aux renseignements personnels qui sont recueillis, utilisés ou communiqués, à l'échelle interprovinciale ou internationale.

Conformément à la LPRPDÉ et aux directives antérieures du Commissaire, la LPVPC ne contient aucune restriction quant au transfert de renseignements personnels à l'extérieur du Canada. Ce régime contraste avec celui prévu à la Loi 64 du Québec et au RGPD, qui prévoient tous les deux une évaluation du niveau d'équivalence du régime étranger de protection des renseignements personnels.

Transparence. La seule exigence prévue à la LPVPC au paragraphe 62(2)(d) est celle de la transparence: la déclaration relative à la protection de la vie privée que les organisations doivent mettre à disposition devra inclure des détails sur le fait que l'organisation effectue ou non un transfert ou une communication internationale ou interprovinciale de renseignements personnels, mais seulement si ce transfert ou cette communication peut avoir des « répercussions raisonnablement prévisibles sur la vie privée ». La dernière portion de cette exigence n'est pas claire et semble sous-entendre que cette déclaration de transparence doit être faite uniquement lorsque des renseignements personnels sont partagés avec une organisation ou une entité qui pourrait être assujettie à des obligations légales étrangères de divulgation (c.-à-d., qui ne peuvent être interdites par contrat) qui ne sont pas substantiellement similaires à celles applicables au Canada.

Coopération avec les autorités étrangères. Reconnaissant la nature internationale inhérente aux efforts de protection des données, l'article 120 de la LPVPC donnera au Commissaire de nouveaux pouvoirs concernant la divulgation de certains renseignements aux législateurs étrangers en matière de protection des renseignements personnels. Il est intéressant de noter que ces pouvoirs incluront la capacité de conclure des accords de coopération avec les autorités étrangères, ce qui peut impliquer: une coopération pour l'application des lois sur la protection des données et la gestion des plaintes, l'élaboration de directives, normes et autres documents relatif à la protection des renseignements personnels, la conduite et la publication de recherches, le partage de connaissance et d'expertise et la détermination de questions d'intérêt commun.

Mesures de sécurité et réponse aux incidents

La LPVPC comprend une obligation de sécurité très semblable à celle qui est actuellement en vigueur en vertu de la LPRPDÉ, soit celle de protéger les renseignements personnels au moyen de mesures de sécurité physiques, organisationnelles et technologiques « proportionnelles » (art. 57(1)). La sensibilité deviendra le nouveau facteur principal régissant le caractère adéquat des mesures de sécurité, bien que « la quantité, […] la répartition, [le] format et […] la méthode de stockage des renseignements » continueront d'être pertinents (art. 57(2)).

Le projet de loi C-27 traite spécifiquement de l'authentification. Les mesures de protection d'une organisation devront comprendre des « mesures raisonnables d'authentification de l'identité de l'individu auquel ces renseignements se rapportent » (par. 57(3)). Nous constatons que le législateur omet de soumettre l'« identification » à cette nouvelle exigence, laquelle consiste à trouver une identité dans une base de données pour déterminer qui est une personne donnée, alors que l'« authentification » consiste plutôt à vérifier ou à confirmer l'identité d'une personne. Ainsi, le projet de loi C-27 insiste sur la mise en place de mesures techniques, organisationnelles et physiques « raisonnables » afin de vérifier ou de confirmer si la personne est bien celle qu'elle prétend être. À cette fin, les organisations devront prêter attention au risque de fraude et de vol d'identité lorsqu'elles évaluent les mesures de protection appropriées à mettre en place pour protéger les renseignements personnels des individus qu'elles authentifient, et tenir compte des bonnes pratiques en matière de sécurité de l'information.

La LPVPC conserve les exigences de notification et de déclaration qui s'appliquent aux mesures de sécurité en cas d' « atteinte à la sécurité » telles qu'elles existent aujourd'hui. Notamment :

- La définition d'« atteinte aux mesures de sécurité » reste inchangée.
- La LPVPC continue d'exiger une déclaration au Commissaire et une notification à l'individu concerné.
- Le seuil de gravité déclenchant l'obligation de déclarations et de notification continue à être celui du « risque réel de préjudice grave ».
- La déclaration et la notification devront être effectuées « dès que possible ».
- L'obligation de notifier les autres organisations dont on estime qu'elles sont en mesure de réduire le risque de préjudice ou d'atténuer le préjudice est maintenue.

La seule nouvelle exigence est que les fournisseurs de services seront obligés, en vertu de la LPVPC, de notifier leurs clients dès que possible après avoir « déterminé qu'une atteinte aux mesures de sécurité s'est produite » (art. 61). Ce changement établit un seuil légal minimum pour la notification des prestataires de services, question généralement régie dans les contrats de fourniture de services. Le seuil de déclenchement choisi pour la notification – une « détermination » – donnera aux fournisseurs le temps d'enquêter sur les incidents de sécurité avant de notifier.

Prochaines étapes

Il est à noter que les employés d'Innovation, Sciences et Développement Économique Canada ont indiqué, lors d'une séance d'information technique au moment de la publication du projet de loi C-27, que les entreprises peuvent s'attendre à une période de transition importante entre l'adoption du projet de loi C-27 et son entrée en vigueur. Par ailleurs, comme le projet prévoit une augmentation considérable des pénalités, il est probable que le gouvernement tiendra des consultations et des audiences afin de recueillir les commentaires des intervenants, comme ce fut le cas récemment au Québec à l'égard de la Loi 64 (voir « *Summary of special consultations and public hearings on Québec's Bill 64* » pour plus de détails (en anglais seulement).

L'équipe Protection de la vie privée et des renseignements personnels de BLG fournira des renseignements supplémentaires sur ce nouveau projet de loi au cours des prochains mois. Nous organiserons des webinaires et préparerons des listes de contrôle et des publications portant sur des questions spécifiques.

Auteurs :

Sep Alavi
T 604.632.3472
salavi@blg.com

Eric Charleston
T 416.367.6566
echarleston@blg.com

Simon Du Perron
T 514.954.2542
SDuperron@blg.com

Daniel-Nicolas El-Khoury
T 514.954.2555
delkhoury@blg.com

Bradley Freedman
T 604.640.4129
bfreedman@blg.com

Julie Gauthier
T 514.954.2555
jugauthier@blg.com

Roberto Ghignone
T 613.369.4791
rghignone@blg.com

Eloïse Gratton
T 416.367.6225
egratton@blg.com

Anthony Hémond
T 514.395.3899
ahemond@blg.com

Elisa Henry
T 514.954.3113
ehenry@blg.com

Max Jarvie
T 514.954.2628
mjarvie@blg.com

François Joli-Coeur
T 514.954.3144
fjolicoeur@blg.com

Dan Michaluk
T 416.367.6097
dmichaluk@blg.com

Shane Morganstein
T 416.367.7281
smorganstein@blg.com

Catherine Labasi-Sammarito
T 514.954.2555
clabasiSammartino@blg.com

Andy Nagy
T 514.395.2714
anagy@blg.com

Katherine Stanger
T 416.367.7294
kstanger@blg.com

Danielle Windt
T 604.640.4120
dwindt@blg.com

blg.com | Vos avocats au Canada

Borden Ladner Gervais