Borden Ladner Gervais

Loi visant à protéger la vie privée et les données des consommateurs (projet de loi C-36) :

ce que les organisations doivent savoir

Juin 2026

Le 15 juin 2026, le ministre de l'Intelligence artificielle et de l'Innovation numérique, Evan Solomon, a déposé le projet de loi C-36, *Loi édictant la Loi visant à protéger la vie privée et les données des consommateurs, modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et apportant des modifications à d'autres lois*.

Cette mesure législative attendue depuis longtemps succède à l'ancien projet de loi C-27, mort au feuilleton en janvier 2025. Le projet de loi C-36 édicte la *Loi visant à protéger la vie privée et les données des consommateurs* (LPVPDC), qui remplace les dispositions relatives à la protection de la vie privée contenues dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

La LPVPDC fait suite à la publication, par le gouvernement fédéral, de L'IA pour tous : Stratégie nationale du Canada en matière d'intelligence artificielle (IA pour tous), dont le premier pilier, « Protéger les Canadiennes et préserver notre système démocratique », souligne que la confiance du public envers l'IA exige des lois modernes en matière de vie privée et de sécurité en ligne, de solides capacités nationales en matière de sûreté de l'IA ainsi que des systèmes gouvernementaux sécurisés, notamment par l'entremise de la *Loi sur les médias sociaux sécuritaires* (projet de loi C-34). Conformément à la stratégie fédérale en matière d'IA, la LPVPDC constitue un cadre juridique modernisé et renforcé en matière de protection de la vie privée et des données au Canada.

Quant à son champ d'application, la LPVPDC demeure essentiellement alignée sur la LPRPDE : elle s'applique à la collecte, à l'utilisation et à la communication de renseignements personnels par une organisation dans le cadre d'activités d'affaires, ainsi qu'aux renseignements personnels des employés à l'égard des entreprises fédérales. Elle est également censée s'appliquer partout au Canada, sauf dans les provinces qui ont adopté des lois sur la protection des renseignements personnels dans le secteur privé essentiellement similaires[1].

BLG a préparé ce guide afin d'expliquer la LPVPDC proposée, de fournir des renseignements pratiques aux organisations et de présenter des éléments de comparaison avec les régimes actuels de protection de la vie privée au Canada et à l'étranger.

Le présent document sera mis à jour au fur et à mesure que le projet de loi franchira les étapes du processus législatif.

Dernière mise à jour : 23 juin 2026

1 Il convient de noter que l'article 139 autorise le gouverneur en conseil à exempter une organisation ou des activités, ainsi que des catégories d'organisations ou d'activités, de l'application de la PPCDA, à condition qu'une loi substantiellement similaire soit applicable dans la province où se trouve l'organisation où se déroulent les activités. Aux fins de cette exemption, le gouverneur en conseil peut prendre des règlements afin de définir les critères et les procédures permettant de déterminer si une loi provinciale est suffisamment similaire.

Table des matières

Ce que vous devez savoir

- Le projet de loi C-36 est actuellement à l'étape initiale du processus législatif, ayant franchi l'étape de la première lecture à la Chambre des communes le 15 juin 2026. À ce jour, il n'existe aucune indication claire quant au moment où il pourrait être adopté et entrer en vigueur.

Un nouveau paradigme d'application de la loi

- La création d'un nouvel organisme de réglementation, la Commission canadienne de la sécurité numérique et de la protection des données, est proposée afin de remplacer le Commissariat à la protection de la vie privée du Canada.
- Des sanctions administratives pouvant atteindre le plus élevé de 10 millions de dollars et de 3 % du revenu mondial.
- Des amendes pour certaines infractions pouvant atteindre le plus élevé de 25 millions de dollars et de 5 % du revenu mondial (pour les actes criminels), ou de 20 millions de dollars et de 4 % du revenu mondial (pour les infractions punissables sur déclaration de culpabilité par procédure sommaire).
- Un nouveau droit privé d'action permettant aux personnes physiques de réclamer des dommages-intérêts pour des contraventions à la LPVPDC dans certaines circonstances.
- Des codes de pratique et des programmes de certification comme nouvel outil volontaire de conformité.

De nouveaux droits individuels, de nouveaux défis opérationnels

- Trois nouveaux droits individuels : le droit d'être informé du recours à la prise de décision automatisée, le droit au retrait et le droit à la mobilité des données.

Des obligations accrues en matière de responsabilité et de gouvernance

- Une clarification selon laquelle les renseignements personnels sont sous le contrôle de l'organisation qui les recueille et qui détermine les fins de leur collecte, de leur utilisation et de leur communication.
- Une nouvelle obligation d'établir, de mettre en œuvre et de rendre accessible un programme de gestion de la protection des renseignements personnels.
- L'établissement du rôle et des responsabilités des fournisseurs de services.

Le consentement simplifié — ou pas?

- Par défaut, le consentement doit être obtenu expressément, sauf lorsque le consentement implicite est approprié.
- De nouvelles exceptions au consentement pour les renseignements dépersonnalisés et les pratiques commerciales légitimes.

Une approche favorable à l'IA

- Des définitions et de nouvelles exigences applicables aux pratiques de dépersonnalisation et d'anonymisation.
- Une exclusion de la plupart des droits individuels pour les renseignements dépersonnalisés.
- Une nouvelle exception au consentement pour la recherche, l'analyse et le développement internes lorsque les renseignements sont dépersonnalisés.
- De nouvelles exigences de transparence applicables à la prise de décision automatisée.

1. Application de la loi

1.1 Nouveau commissaire (art. 76)

Le Commissariat à la protection de la vie privée du Canada (CPVP) ne serait plus responsable de superviser le régime fédéral de protection des renseignements personnels dans le secteur privé. Il serait plutôt remplacé par la nouvelle Commission canadienne de la sécurité numérique et de la protection des données (la Commission), également créée par la *Loi sur la sécurité numérique* (projet de loi C-34). La Commission se compose de cinq membres nommés par le gouverneur en conseil, dont l'un est désigné comme commissaire à la protection de la vie privée et des données des consommateurs (le commissaire).

Avec ce changement majeur, le projet de loi C-36 centralise l'application fédérale des lois en matière de protection des renseignements personnels au sein d'un seul organisme de réglementation chargé plus largement de l'application des lois liées au numérique. Ce modèle diffère de ceux du Québec, de l'Union européenne et du Royaume-Uni, où l'application des lois en matière de protection des renseignements personnels relève de commissaires responsables de la protection des données.

Il s'écarte également de l'approche proposée dans le projet de loi C-27, qui aurait créé un tribunal distinct chargé d'imposer des sanctions administratives pécuniaires. Sous le régime du projet de loi C-36, la nouvelle Commission a le pouvoir d'imposer des sanctions administratives pécuniaires, sous réserve de mécanismes de révision et d'appel devant la Cour fédérale.

Nomination. Le modèle de nomination du nouveau commissaire marque également un changement institutionnel important. Dans le cadre actuel, le commissaire à la protection de la vie privée du Canada est un agent du Parlement, nommé avec l'approbation de la Chambre des communes et du Sénat, et relève directement du Parlement. Ce modèle vise à renforcer l'indépendance du commissaire par rapport au gouvernement.

Le projet de loi C-36 prévoit plutôt que le commissaire serait nommé par le gouverneur en conseil (en pratique, le cabinet), ce qui pourrait soulever des questions quant à l'indépendance institutionnelle du nouveau régulateur, compte tenu notamment de ses pouvoirs d'application accrus et de son mandat réglementaire élargi pour tout ce qui est numérique.

Perte d'une voix réglementaire pragmatique et de confiance. Au fil du temps, le CPVP a développé une expertise pratique qui dépasse le rôle traditionnel d'application de la loi. Il a notamment acquis une capacité consultative significative auprès des organisations du secteur privé, appuyée par des ressources expérimentées et une solide compréhension des réalités opérationnelles.

De plus, le CPVP joue aussi un rôle actif dans les forums internationaux sur la protection de la vie privée, notamment le Global Privacy Enforcement Network et la table ronde des autorités de protection des données du G7. Ces activités favorisent l'harmonisation avec les tendances mondiales et renforcent la capacité du CPVP à traiter les enjeux transfrontaliers.

Dans une économie fondée sur les données, où l'application de la loi vise de plus en plus des organisations multinationales, des fournisseurs mondiaux et des flux transfrontaliers de renseignements, cette expérience internationale peut également favoriser une plus grande cohérence dans l'interprétation et l'application du droit canadien de la protection des renseignements personnels. La transition vers un nouveau régulateur comporte donc un risque réel que cette expertise accumulée, développée au fil du temps par la pratique, la consultation et la coopération internationale, soit difficile à reproduire dans un nouveau cadre réglementaire.

Pouvoirs actuels maintenus. La LPVPDC reprend certains pouvoirs prévus par la LPRPDE, notamment la possibilité pour les personnes de déposer des plaintes et celle pour le commissaire d'entreprendre une plainte de sa propre initiative. Le commissaire conserve également les pouvoirs suivants :

- Mener des enquêtes relativement à une plainte;
- Conclure des accords de conformité avec les organisations qui ont contrevenu à la loi;
- Effectuer des vérifications portant sur la conformité d'une organisation à la loi.

La LPVPDC maintiendrait également le pouvoir du CPVP de publier des lignes directrices et de fournir des services consultatifs aux organisations qui en font la demande.

Nouveaux pouvoirs. La LPVPDC confère également au commissaire d'importants nouveaux pouvoirs lui permettant de rendre des ordonnances de conformité lorsqu'il l'estime raisonnablement nécessaire pour assurer le respect de la Loi. Ces ordonnances peuvent contraindre les organisations en défaut à :

- Prendre les mesures nécessaires pour se conformer à la loi;
- Cesser de faire quelque chose qui contrevient à la loi;
- Respecter un accord de conformité;
- Rendre publiques les mesures visant à corriger ses politiques, pratiques ou procédures.

Il est également intéressant de noter que la Commission et le commissaire doivent tenir compte de l'intérêt supérieur des enfants, ainsi que de l'importance de soutenir la croissance économique, la concurrence et l'innovation sur le marché canadien lorsqu'ils exercent leurs pouvoirs.

1.2 Sanctions pécuniaires (art. 113, 145)

Dans le cadre de l'avis de contravention, le commissaire doit également décider s'il y a lieu d'imposer une sanction, comme le font les autorités de protection de la vie privée sous d'autres régimes, notamment le RGPD et la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (Loi sur le secteur privé)[2].

Contraventions. Des sanctions pouvant atteindre le plus élevé de 10 000 000 $ et de 3 % du revenu mondial brut de l'organisation peuvent être imposées pour des contraventions relatives aux éléments suivants :

- Mettre en œuvre un programme adéquat de gestion de la protection des renseignements personnels;
- Transférer des renseignements personnels à un fournisseur de services;
- Veiller à ce que les renseignements personnels soient recueillis, utilisés et communiqués à des fins appropriées;
- Limiter la collecte, l'utilisation et la communication de renseignements personnels;
- Obtenir le consentement pour une nouvelle fin;
- Obtenir un consentement valide;
- Expliquer les conséquences du retrait du consentement;

2 Voir l'article 58(2)(i) du RGPD et l'article 90.1 de la Loi sur le secteur privé du Québec.

- Conserver les renseignements personnels uniquement pendant les périodes nécessaires;
- Retirer les renseignements personnels à la demande d'une personne;
- Veiller à ce que les fournisseurs de services suppriment les renseignements personnels lorsque ceux-ci leur ont été transférés;
- Protéger les renseignements personnels au moyen de mesures de sécurité;
- Déclarer les atteintes aux mesures de sécurité à la Commission et à la personne concernée;
- Faire en sorte que les fournisseurs de services avisent l'organisation en cas d'atteinte; et
- Rendre les politiques et procédures facilement accessibles et rédigées en langage clair.

Infractions. Pour les actes criminels, des sanctions pouvant atteindre le plus élevé de 25 000 000 $ ou 5 % du revenu mondial brut de l'organisation peuvent être imposées, ou, pour les infractions punissables sur déclaration de culpabilité par procédure sommaire, des sanctions pouvant atteindre le plus élevé de 20 000 000 $ ou 4 % du revenu mondial brut de l'organisation, si l'organisation, sciemment :

- Ne déclare pas une atteinte aux mesures de sécurité à la Commission;
- Ne tient pas de registres des atteintes aux mesures de sécurité;
- Ne conserve pas les renseignements personnels pendant une période suffisante dans le contexte d'une demande d'accès;
- Utilise des renseignements dépersonnalisés dans des circonstances interdites;
- Contrevient à une ordonnance de la Commission rendue à la suite d'un avis de contravention;
- Défavorise un dénonciateur.

1.3 Appels (art. 126 à 128)

La LPVPDC accorde aux plaignants et aux organisations un droit d'appel devant la Cour fédérale à l'encontre de toute décision du commissaire concluant que l'organisation a contrevenu, ou n'a pas contrevenu, à la LPVPDC. Les demandes doivent être présentées dans les 30 jours suivant la décision.

1.4 Droit privé d'action (art. 132)

La LPVPDC introduit un nouveau droit privé d'action.

Les personnes touchées par une contravention à la LPVPDC peuvent intenter une action contre l'organisation afin d'obtenir des dommages-intérêts pour compenser la perte ou le préjudice subi en raison de cette contravention, pourvu que : a) le commissaire ait conclu que l'organisation a contrevenu à la LPVPDC et que cette conclusion soit définitive; b) la Cour fédérale ait conclu que l'organisation a contrevenu à la LPVPDC; c) une décision définitive rejetant tout appel ou confirmant la contravention ait été rendue et que tous les droits d'appel aient été épuisés; ou d) le commissaire ait conclu un accord de conformité avec l'organisation.

La LPVPDC confère également aux personnes un droit privé d'action contre l'organisation déclarée coupable d'une infraction prévue à l'article 145 de la LPVPDC.

Dans chaque cas, le droit privé d'action doit être exercé dans les deux ans suivant la date à laquelle la personne prend connaissance de la conclusion du commissaire, de la décision de révision ou de la décision d'appel.

Contrairement à la Loi sur le secteur privé du Québec, qui prévoit des dommages-intérêts statutaires dans certaines circonstances à l'article 93.1, la LPVPDC ne crée pas de régime de dommages-intérêts statutaires, ce qui peut signifier que le risque d'actions collectives en matière de protection des renseignements personnels intentées devant la Cour fédérale demeurerait marginal par rapport à ce que l'on observe actuellement au Québec.

1.5 Dénonciation et dispositions anti-représailles (art. 143 et 144)

La LPVPDC maintient la protection des dénonciateurs actuellement prévue par la LPRPDE. Le commissaire a utilisé des renseignements reçus en vertu de cette disposition pour entreprendre une plainte à au moins une occasion (Résumé de conclusions en vertu de la LPRPDE no 310). La LPVPDC comprend également une disposition anti-représailles qui reprend celle prévue par la LPRPDE.

1.6 Codes de pratique et programmes de certification (art. 92 à 96)

La LPVPDC prévoit la création de « codes de pratique » et de « programmes de certification » comme moyen d'encourager des pratiques volontaires et sectorielles favorisant la protection des renseignements personnels. Des dispositions similaires figurent aux articles 40 à 43 du RGPD et pourraient accroître la prévisibilité dans l'application de la LPVPDC.

Afin d'encourager davantage l'élaboration de pratiques améliorées et cohérentes en matière de protection des renseignements personnels, la LPVPDC permettra à toute organisation, assujettie ou non à la LPVPDC, ainsi qu'aux institutions gouvernementales, de demander au commissaire d'approuver des codes de pratique et des programmes de certification. L'organisation pourra choisir de s'y conformer volontairement et de maintenir sa certification afin de réduire les risques liés à la non-conformité à la LPVPDC et de mettre en valeur son engagement à l'égard de la conformité en matière de protection des renseignements personnels. Toutefois, cela ne constituera pas nécessairement une preuve de conformité complète à la LPVPDC.

Aucune sanction pour contravention à la LPVPDC ne doit être imposée si l'organisation, au moment de la contravention, se conformait aux exigences d'un programme de certification approuvé par la Commission. Cette règle d'exonération souligne la valeur des codes de pratique approuvés comme mécanisme stratégique de conformité pour les organisations.

2. Responsabilité et gouvernance

La LPVPDC codifie et précise le principe de responsabilité actuellement énoncé à l'annexe 1 de la LPRPDE. Bien que les changements apportés aux exigences actuelles semblent relativement limités, certaines additions notables prévues par la LPVPDC devraient accroître la clarté de ces exigences pour les organisations.

2.1 Notion de contrôle (art. 7)

Comme sous le régime de la LPRPDE, la LPVPDC prévoit qu'une organisation est responsable des renseignements personnels dont elle a le contrôle. La LPVPDC va cependant plus loin en indiquant que les renseignements personnels « relèvent » de l'organisation qui décide de les recueillir et qui détermine les fins de leur collecte, de leur utilisation ou de leur communication. La LPVPDC précise clairement qu'une organisation conserve le contrôle des renseignements personnels même lorsqu'elle les transfère à un fournisseur de services, ou lorsque les renseignements sont recueillis, utilisés ou communiqués par un fournisseur de services pour le compte de l'organisation.

À l'instar du RGPD, la LPVPDC distingue les obligations applicables à l'organisation qui contrôle les renseignements personnels de celles applicables aux fournisseurs de services, ces derniers n'étant pas assujettis à la partie I de la LPVPDC, qui traite des obligations de l'organisation, sauf en ce qui concerne les mesures de sécurité et l'avis aux clients en cas d'atteinte.

2.2 Rôle du responsable de la protection des renseignements personnels (art. 8)

Sous le régime de la LPVPDC, l'organisation doit désigner une personne chargée de veiller au respect des obligations de l'organisation prévues par la Loi, rôle généralement appelé « responsable de la protection des renseignements personnels ». L'organisation doit également fournir les coordonnées professionnelles de la personne désignée à toute personne qui en fait la demande. La LPVPDC ne précise pas qui, au sein de l'organisation, doit exercer ce rôle.

2.3 Programme de gestion de la protection des renseignements personnels (art. 9)

La LPVPDC exigera que chaque organisation mette en œuvre et maintienne un programme de gestion de la protection des renseignements personnels comprenant les politiques, les pratiques et les procédures qu'elle applique pour satisfaire à ses obligations au titre de la LPVPDC.

Le contenu obligatoire de ces politiques est généralement le même que sous le régime de la LPRPDE : elles doivent traiter de la protection des renseignements personnels, du traitement des demandes de renseignements et des plaintes, de la formation du personnel sur les politiques et procédures, ainsi que de l'élaboration de documents expliquant ces politiques et procédures.

Il est à noter que la LPVPDC introduit une nouvelle exigence selon laquelle une organisation doit tenir compte du volume et du caractère sensible des renseignements personnels dont elle a le contrôle lorsqu'elle élabore son programme de gestion de la protection des renseignements personnels. Cette exigence vise

vraisemblablement à renforcer le message que le commissaire répète depuis longtemps, soit que les politiques et les mesures de protection de l'organisation doivent être raisonnables compte tenu des types de renseignements qu'elle traite.

La LPVPDC exigera également qu'une organisation donne accès au commissaire à ses politiques, ses pratiques et ses procédures sur demande. Bien que la LPRPDE ne contienne pas d'exigence équivalente, l'organisation fournit généralement de tels documents au CPVP dans tous les cas. Après avoir examiné ces documents, la LPVDC ajoute désormais que le commissaire peut formuler des conseils ou recommander la prise de mesures correctives.

2.4 Registre des fins (art. 12)

La LPVPDC exige par ailleurs qu'une organisation identifie et consigne chacune des fins auxquelles elle recueille, utilise ou communique des renseignements personnels au moment de la collecte ou avant celle-ci.
Si l'organisation décide que les renseignements personnels recueillis doivent être utilisés ou communiqués à une nouvelle fin, elle doit consigner cette nouvelle fin avant d'utiliser ou de communiquer les renseignements à cette nouvelle fin.

À l'heure actuelle, la LPRPDE repose sur une obligation plus souple, fondée sur des principes, d'identifier et de documenter les fins, sans exiger un inventaire complet des données. Cette exigence rapproche la LPVPDC de l'obligation de tenue de registre prévue à l'article 30 du RGPD, qui exige un registre formel et structuré des activités de traitement.

En pratique, cette exigence pourrait s'avérer lourde pour les organisations qui recueillent des renseignements personnels à une multitude de fins, d'autant plus que les meilleures pratiques exigent la tenue d'un registre adéquat des journaux.

3. Consentement

La LPVPDC apporte des modifications importantes à la notion de consentement en introduisant une exception au consentement pour certaines activités d'affaires déterminées, ainsi qu'une exception plus souple pour certaines opérations de traitement effectuées dans le cadre d'une activité à l'égard de laquelle l'organisation possède un « intérêt légitime ».

Ce faisant, la LPVPDC s'éloigne du modèle centré sur le consentement, souvent critiqué, qui caractérise le régime législatif fédéral actuel, et ce, au profit d'une approche plus équilibrée reconnaissant que le consentement n'est ni réaliste ni raisonnable dans toutes les circonstances. En somme, la LPVPDC cherche à établir un meilleur équilibre entre les intérêts commerciaux légitimes de l'organisation dans le traitement des renseignements personnels et les droits à la vie privée des Canadiens.

3.1 Forme du consentement (art. 15)

Le consentement exprès constitue la forme de consentement par défaut sous le régime de la LPVPDC, mais une organisation peut s'appuyer sur un consentement implicite si cela est « approprié » dans les circonstances, compte tenu des « attentes raisonnables de la personne » et de la « sensibilité » des renseignements personnels.

Bien que la première notion ne soit pas définie expressément dans la loi, la LPVPDC ajoute une nouvelle définition de « renseignement sensible », inspirée du bulletin d'interprétation du CPVP sur les renseignements sensibles. Cette définition inclut les renseignements personnels des enfants, ce qui renforce la norme de consentement applicable à ce type particulier de renseignements. Pour les autres types de renseignements, la sensibilité devra être évaluée de façon contextuelle.

Il est également intéressant de noter que, comparativement à la façon dont le CPVP définissait les renseignements sensibles dans son bulletin d'interprétation[3], la définition de la LPVPDC n'inclut pas les renseignements financiers, ce qui indique clairement que le législateur entend préserver une approche contextuelle à l'égard de ce type de renseignements.

La LPVPDC 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. En particulier, la LPVPDC établit une règle selon laquelle le consentement implicite est réputé inapproprié si la collecte ou l'utilisation de renseignements personnels est effectuée dans le cadre d'une activité relevant de la nouvelle exception au consentement visant certaines activités d'affaires déterminées, ou d'activités à l'égard desquelles l'organisation possède un intérêt légitime.

Ces distinctions semblent renforcer la notion de consentement en obligeant l'organisation à s'appuyer sur l'une des exceptions au consentement mentionnées ci-dessus, ou à obtenir un consentement exprès pour une ou plusieurs des activités décrites dans ces dispositions. Toutefois, compte tenu de l'étendue des activités susceptibles d'être visées par l'exception relative à l'intérêt légitime (analysée plus loin à la section 3.4), les situations dans lesquelles une organisation peut s'appuyer sur le consentement implicite sans d'abord réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) conformément à l'alinéa 18(4)b) de la LPVPDC demeurent ambiguës (comme il est expliqué plus en détail ci-dessous).

3 « Certaines catégories de renseignements personnels seront généralement considérées comme sensibles et doivent faire l'objet d'une meilleure protection – notamment les renseignements sur la santé, les finances, les origines ethniques et raciales, les opinions politiques, la vie sexuelle ou l'orientation sexuelle et les croyances religieuses ou philosophiques, les données génétiques, les données neuronales ainsi que les données biométriques permettant d'identifier précisément une personne. »

On peut s'attendre à ce que la portée et l'application du paragraphe 15(6) de la LPVPDC soient précisées au fur et à mesure que le projet de loi C-36 avancera dans le processus législatif.

3.2 Avis de confidentialité et consentement éclairé (art. 15)

Renseignements à fournir. Quelle que soit la forme du consentement, l'organisation doit fournir certains types de renseignements à la personne dont le consentement est sollicité afin de s'assurer que son consentement soit suffisamment éclairé. La LPVPDC exige que les éléments suivants soient fournis au moment où le consentement est sollicité ou avant celui-ci :

- Les fins auxquelles les renseignements personnels sont traités;
- La manière dont les renseignements personnels sont traités;
- Toute conséquence raisonnablement prévisible découlant des opérations de traitement;
- Le type précis de renseignements personnels devant être traités;
- Le nom des tiers ou les catégories de tiers auxquels les renseignements personnels peuvent être communiqués.

Ces exigences reflètent étroitement les lignes directrices du CPVP sur l'obtention d'un consentement valable, mais semblent aller plus loin que les lignes directrices québécoises sur le consentement, notamment par l'exigence expresse de communiquer toute conséquence raisonnablement prévisible découlant du traitement. La portée de cette exigence devra être précisée, y compris la question de savoir si elle s'étend aux conséquences comportementales ou aux effets liés à l'influence, compte tenu notamment de l'objectif stratégique plus large du gouvernement fédéral visant à encadrer les pratiques de surveillance fondées sur les données, comme l'indique sa stratégie IA pour tous.

Format. La LPVPDC précise maintenant que les renseignements décrits ci-dessus doivent non seulement être fournis dans un « langage clair », mais aussi dans un langage suffisamment adapté au public cible, de sorte qu'il serait raisonnable de s'attendre à ce que celui-ci « comprenne » le contenu de l'avis. Cette exigence s'inscrit largement dans la continuité de l'article 6.1 de la LPRPDE.

Une question importante que le projet de loi C-36 laisse essentiellement sans réponse demeure la manière et le format précis selon lesquels cet avis doit être présenté à une personne. Par exemple, les outils souvent utilisés par l'organisation pour présenter le contenu de façon pratique et accessible, comme les avis par couches et les avis contextuels, ne sont pas mentionnés expressément, malgré la recommandation du CPVP d'utiliser de tels mécanismes dans son bulletin d'interprétation. Bien que les règles relatives au format, à la structure du contenu et à l'accessibilité des renseignements demeurent imprécises, l'organisation doit néanmoins tenir compte des difficultés susceptibles de découler du contexte global dans lequel le consentement est sollicité lorsqu'elle détermine comment fournir les renseignements pertinents ou y diriger activement les personnes.

Pratiques trompeuses. L'article 16 renforce davantage le cadre de consentement de la LPVPDC en prévoyant qu'une organisation ne doit pas obtenir, ni tenter d'obtenir, le consentement d'une personne en lui fournissant des renseignements faux ou trompeurs, ou en ayant recours à des pratiques trompeuses ou mensongères. Sinon, tout consentement obtenu dans de telles circonstances est invalide.

Ces pratiques ne sont pas définies expressément dans la Loi. Toutefois, le projet de loi C-36 emploie un langage s'alignant étroitement avec le rapport du CPVP de 2024 sur les conceptions trompeuses, qui décrit ces pratiques comme des choix de conception utilisés sur des sites Web et des applications pour influencer, manipuler ou contraindre les utilisateurs à prendre des décisions qui ne sont pas dans leur intérêt, et qui

peuvent les empêcher de faire des choix éclairés concernant la collecte, l'utilisation et la communication de leurs renseignements personnels. Il reprend également un vocabulaire plus large issu du droit de la protection du consommateur, notamment de la *Loi sur la concurrence* et des lois sur la protection du consommateur[4]. Il sera intéressant de suivre l'interprétation de cette disposition à l'égard des parcours de consentement et des bannières de témoins.

3.3 Retrait du consentement et autres exigences clés (art. 15)

La LPVPDC maintient largement le statu quo à l'égard de certaines autres exigences clés liées au consentement prévues par la LPRPDE. 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 pas constituer une condition de service (caractère facultatif du consentement); une personne a le droit de retirer son consentement en tout temps, sous réserve d'un préavis raisonnable, du droit applicable ou des modalités raisonnables d'un contrat (retrait du consentement); et le consentement demeure invalide s'il a été obtenu au moyen de renseignements faux ou trompeurs, ou de pratiques trompeuses ou induisant en erreur (consentement obtenu par tromperie).

3.4 Nouvelles exceptions au consentement (art. 18, 20 à 22)

La plupart des exceptions au consentement prévues par la LPRPDE sont reprises dans la LPVPDC, avec des modifications limitées. La LPVPDC introduit plusieurs nouvelles exceptions au consentement, notamment pour certaines activités d'affaires déterminées, ainsi qu'une exception plus souple lorsque l'organisation a un intérêt légitime qui « l'emporte sur tout effet négatif raisonnablement prévisible sur la personne » découlant de la collecte ou de l'utilisation de ses renseignements personnels.

Ces exceptions, ainsi que quelques autres introduites pour les renseignements personnels dépersonnalisés, sont examinées plus en détail ci-dessous.

Exception visant les activités d'affaires déterminées. Une organisation peut recueillir ou utiliser des renseignements personnels à l'insu de la personne et sans son consentement si ce traitement est effectué aux fins d'une activité d'affaires déterminée, autre que l'influence du comportement ou des décisions de la personne (ce qui inclut vraisemblablement la publicité et le marketing), et s'inscrit dans les attentes raisonnables de la personne.

En particulier, la LPVPDC précise que les activités suivantes constituent des « activités d'affaires » :

- La fourniture d'un produit ou d'un service demandé par la personne à l'organisation;
- La sécurité des renseignements, des systèmes ou des réseaux de l'organisation;
- La sécurité d'un produit ou d'un service fourni par l'organisation; et
- Toute autre activité prévue par règlement.

L'exclusion des activités réalisées dans le but d'influencer le comportement ou les décisions d'une personne pourrait s'avérer particulièrement importante dans le contexte de la publicité, des témoins de navigation et des technologies de suivi similaires.

Puisqu'on pourrait soutenir que la finalité de la publicité consiste à influencer les décisions d'une personne, il pourrait être avancé que les organisations ne devraient pas pouvoir s'appuyer sur cette exception pour les

4 Par exemple, voir l'article 219 de la Loi sur la protection du consommateur au Québec.

témoins utilisés à des fins de publicité comportementale, de personnalisation, de reciblage ou à d'autres fins orientées vers l'influence. En pratique, cette hypothèse signifierait que le consentement exprès demeurera vraisemblablement requis pour la publicité (et, en ligne, pour de nombreux témoins non essentiels), même lorsque l'organisation pourrait autrement soutenir que l'activité appuie ses activités d'affaires et s'inscrit dans les attentes raisonnables de la personne.

Une exclusion similaire est également prévue pour la collecte d'adresses électroniques au moyen de programmes informatiques conçus ou commercialisés principalement pour générer, rechercher ou recueillir des adresses électroniques. De telles activités exigeront le consentement explicite des personnes.

Exception relative à l'intérêt légitime. L'ajout d'une nouvelle exception souple relative à l'intérêt légitime pour la collecte ou l'utilisation de renseignements personnels à l'insu de la personne et sans son consentement constitue un développement important. En particulier, une organisation peut s'appuyer sur cette exception lorsque les renseignements personnels sont recueillis, utilisés ou communiqués aux fins d'une activité à l'égard de laquelle (i) l'organisation possède un intérêt légitime qui l'emporte sur tout effet négatif raisonnablement prévisible sur la personne découlant de la collecte, de l'utilisation ou de la communication; (ii) les renseignements personnels ne sont pas recueillis, utilisés ou communiqués dans le but d'influencer le comportement ou les décisions de la personne; et (iii) ce traitement s'inscrit dans les attentes raisonnables de la personne.

Conformément aux appels des autorités de protection de la vie privée voulant qu'un pouvoir accru d'utiliser des renseignements personnels s'accompagne d'une responsabilité accrue des organisations, une organisation doit, avant de s'appuyer sur cette exception :

- Identifier l'intérêt légitime;
- Réaliser et consigner une EFVP et, sur demande, en fournir une copie au commissaire fédéral à la protection de la vie privée;
- Identifier les mesures raisonnables mises en œuvre pour réduire la probabilité que les effets se produisent, ou pour les atténuer ou les éliminer;
- Démontrer le respect de toute autre exigence prévue par règlement.

Même si une organisation qui s'appuie sur cette exception peut recueillir et utiliser des renseignements personnels à l'insu de la personne et sans son consentement, il convient de noter qu'elle doit néanmoins faire preuve de transparence dans sa politique de confidentialité quant à la manière dont elle applique les exceptions au consentement, notamment en fournissant une description de toute activité relevant de l'exception relative à l'intérêt légitime.

Bien qu'elle soit semblable à la notion d'intérêt légitime prévue par le RGPD, l'exception relative à l'intérêt légitime de la LPVPDC demeure précisément cela : une exception à la notion de consentement, et non une autre base juridique autonome de traitement des renseignements placée sur un pied d'égalité avec le consentement. Toutefois, contrairement au RGPD, cette exception ne permet pas expressément de tenir compte de l'intérêt légitime d'une autre personne (c'est-à-dire autre que celui de l'organisation qui recueille ou utilise les renseignements).

À ce stade, il n'est pas clair quels types précis d'activités pourraient ou non relever de l'« intérêt légitime » d'une organisation et, en particulier, si cela pourrait s'étendre à l'amélioration de produits, au développement de nouveaux produits ou services, voire à certaines formes de publicité ou de marketing, comme le marketing direct ou la publicité géolocalisée.

Renseignements accessibles au public. Sous le régime de la LPVPDC, les renseignements accessibles au public et précisés par règlement peuvent être recueillis, utilisés ou communiqués sans consentement. Cette nouvelle exception pourrait ouvrir la porte à des débats d'interprétation semblables à ceux soulevés dans l'affaire *Clearview AI Inc v. Alberta (Information and Privacy Commissioner)*, 2025 ABKB 287.

Communication à un avocat ou un notaire. Comme sous le régime de la LPRPDE, la LPVPDC permet à une organisation de communiquer des renseignements personnels sans consentement à un avocat ou un notaire. En revanche, la Loi sur le secteur privé du Québec adopte une approche plus large[5]. Bien qu'elle exige généralement une entente écrite lorsque des renseignements personnels sont communiqués à un fournisseur de services, elle dispense les membres d'un ordre professionnel de l'obligation de préciser, dans cette entente, les mesures devant être prises pour protéger les renseignements personnels. Par conséquent, sous le régime de la LPVPDC, les communications à des membres d'un ordre professionnel autres que des avocats ou des notaires exigeraient toujours des protections contractuelles appropriées, alors que le droit québécois dispenserait ces professionnels des exigences relatives au contenu prescrit des ententes avec des tiers.

Exceptions particulières applicables aux renseignements personnels dépersonnalisés. En plus de permettre l'utilisation de renseignements personnels à l'insu de la personne et sans son consentement aux fins de dépersonnalisation, la LPVPDC offre à l'organisation les exceptions au consentement suivantes pour les renseignements dépersonnalisés :

- **Exception relative à la recherche, à l'analyse et au développement internes.** Une organisation peut utiliser des renseignements dépersonnalisés à des fins internes de recherche, d'analyse et de développement (art. 21 LPVPDC). Il s'agit d'une permission large, susceptible d'inciter les organisations à dépersonnaliser les renseignements personnels afin d'en permettre une utilisation interne plus étendue, y compris pour des activités ayant une valeur commerciale.

- **Transaction commerciale éventuelle.** Bien que la LPVPDC exige que les parties à une transaction commerciale éventuelle dépersonnalisent les renseignements personnels (entre autres exigences) afin de les utiliser ou de les communiquer à l'insu de la personne et sans son consentement, cette exigence a été atténuée.

  En particulier, l'organisation n'est pas tenue de dépersonnaliser les renseignements avant leur utilisation ou leur communication si cela devait compromettre les objectifs de la transaction, et si l'organisation a tenu compte du risque de préjudice découlant de ce traitement. Par exemple, pendant la phase de vérification diligente d'une transaction, il est nécessaire de connaître l'identité de certaines personnes, comme les personnes occupant des postes décisionnels ou stratégiques, ou les employés clés, notamment aux fins de recherches publiques, de vérification des conflits d'intérêts ou de vérification des antécédents.

  Ces exigences montrent la nécessité de prévoir des protections contractuelles particulières dès l'étape de la lettre d'intention, en plus de celles relatives à l'utilisation, à la protection, ainsi qu'au retour ou à la destruction des renseignements reçus avant la clôture d'une transaction. En pratique, sans cette exception, l'exigence serait difficile à respecter alors que les échéanciers transactionnels sont souvent serrés et que les vendeurs sont fréquemment de plus petites entreprises, disposant de moins de ressources.

5 Voir article 18.3.

3.5 Fins appropriées (art. 12)

La LPRPDE comprend un critère général de raisonnabilité (c'est-à-dire le critère de la « personne raisonnable »), qui délimite son application et qui peut s'appliquer même si le consentement a été obtenu auprès des personnes. La LPVPDC comprend une exigence similaire selon laquelle une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels que de manière et à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances.

Bien que cette disposition de la LPVPDC, dans le projet de loi C-36, soit semblable à celle prévue par la LPRPDE, les mots « de manière » ont été ajoutés dans le projet de loi C-36, qui précise également que ce critère de raisonnabilité s'applique « que le consentement soit ou non requis sous le régime de la présente loi ».

La LPVPDC énonce les facteurs dont il faut tenir compte pour déterminer si la manière et les fins sont appropriées. Ces facteurs sont largement les mêmes que ceux élaborés dans la décision *Turner c. Telus Communications Inc.*, dans laquelle la Cour fédérale, puis la Cour d'appel fédérale, ont établi les facteurs permettant d'évaluer si la fin poursuivie par une organisation respecte le paragraphe 5(3)[6]. Ces facteurs sont les suivants :

- La sensibilité des renseignements personnels;
- La correspondance des fins aux besoins commerciaux légitimes de l'organisation;
- L'efficacité de la collecte, de l'utilisation ou de la communication pour répondre aux besoins commerciaux légitimes de l'organisation;
- L'existence de moyens moins intrusifs d'atteindre ces fins à un coût comparable et avec des avantages comparables;
- La proportionnalité entre la perte de vie privée de la personne et les avantages, compte tenu des mesures, techniques ou autres moyens mis en œuvre par l'organisation pour atténuer les effets de cette perte de vie privée sur la personne.

Comme indiqué plus haut (voir la section 2.4), sous le régime de la LPVPDC, chacune des fins auxquelles les renseignements personnels doivent être recueillis, utilisés ou communiqués doit être déterminée et consignée au moment de la collecte ou avant celle-ci.

6 Voir aussi le guide du CPVP : Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3).

4. Droits individuels

La LPVPDC reconnaît formellement la vie privée comme un « droit fondamental ».

Comme sous le régime de la LPRPDE, la LPVPDC accorde aux personnes le droit d'accéder à leurs renseignements personnels et les faire rectifier. La LPVPDC confère également aux personnes de nouveaux droits relatifs à la prise de décision automatisée, au retrait des données et à la mobilité des données dans certaines circonstances précises. Il importe de souligner que la LPVPDC exclut expressément les renseignements personnels dépersonnalisés de certains droits individuels prévus par la LPVPDC, mais non de tous.

4.1 Droit d'accès et de rectification (art. 63 à 71)

Droit d'accès. Comme sous le régime de la LPRPDE, la LPVPDC confère aux personnes le droit de connaître et d'avoir accès aux renseignements personnels qui sont détenus par une organisation à leur sujet.

Sur demande écrite, une organisation doit informer la personne, dans un langage clair :

- Si elle détient des renseignements personnels à son sujet;
- La façon dont elle utilise ces renseignements;
- Si elle les a communiqués et, le cas échéant, le nom ou les types de tiers concernés, y compris pour les communications faites sans consentement.

Elle doit également donner accès aux renseignements eux-mêmes. La LPRPDE permet à une organisation de fournir à une personne une liste des tiers auxquels elle peut avoir communiqué ses renseignements personnels lorsqu'il n'est pas possible de fournir une liste exacte des tiers auxquels la communication a été faite. Cette option est notamment absente de la LPVPDC.

Droit de rectification. Comme sous le régime de la LPRPDE, la LPVPDC confère aux personnes le droit de faire rectifier leurs renseignements personnels. L'organisation doit modifier les renseignements que la personne démontre être inexacts, désuets ou incomplets. Le cas échéant, l'organisation doit également transmettre les renseignements modifiés à tout tiers qui y a accès.

Si l'organisation n'est pas d'accord avec les modifications demandées, elle doit consigner le désaccord et, le cas échéant, en informer tout tiers qui a accès aux renseignements.

Il est intéressant de noter que le droit de rectification semble être lié au droit d'accès, puisque le paragraphe 71(1) de la LPVPDC subordonne le droit de rectification au fait que la personne ait d'abord eu accès à ses renseignements personnels. Cela constituerait un écart par rapport à la LPRPDE, sous le régime de laquelle le droit de rectification existait comme un droit autonome. Toutefois, il est peu probable que le législateur ait voulu limiter les demandes de correction aux situations où le droit d'accès a été formellement exercé, puisqu'une personne qui croit qu'une organisation détient des renseignements inexacts pourrait raisonnablement invoquer l'article 55 de la LPVPDC (exactitude des renseignements) et l'obligation générale de l'organisation de veiller à ce que les renseignements personnels soient exacts.

4.2 Droit à la mobilité des données (art. 72 et 140)

La LPVPDC innove à l'article 72 en créant un droit limité à la portabilité des données, qui permettra aux personnes de demander qu'une organisation communique, dès que possible, à une organisation tierce désignée par la personne, les renseignements que la première organisation a recueillis auprès de la personne, pourvu que les deux organisations soient assujetties à un « cadre de mobilité des données ». Il importe de souligner que le droit à la mobilité ne vise que les renseignements personnels que l'organisation recueille auprès des personnes elles-mêmes (c'est-à-dire non auprès de tiers).

Cadres de mobilité des données. La LPVPDC permet au gouverneur en conseil de prendre des règlements qui :

- Établissent les mesures de sécurité que l'organisation doit mettre en place pour assurer la communication et la collecte sécuritaires de renseignements personnels, ainsi que les paramètres techniques nécessaires pour assurer l'interopérabilité entre les systèmes;
- Précisent quelles organisations sont assujetties à un cadre de mobilité des données;
- Créent des exceptions à l'obligation de communication, notamment pour protéger des renseignements commerciaux exclusifs ou confidentiels.

Le droit à la mobilité prévu par la LPVPDC est plus restreint que ceux prévus par la Loi sur le secteur privé du Québec et le RGPD, puisque ces deux droits à la portabilité s'appliquent généralement, sans restreindre les organisations pouvant faire l'objet de demandes de mobilité des données. Par conséquent, la LPVPDC n'ouvre pas entièrement la porte aux demandes générales de portabilité prévues par la Loi sur le secteur privé du Québec et le RGPD.

Bien qu'elle soit assujettie à des règles différentes, la récente *Loi sur les services bancaires axés sur les consommateurs* (projet de loi C-15) peut être considérée comme une application sectorielle de ce droit plus large à la mobilité des données. Ensemble, ces deux régimes de mobilité des données contribuent à l'objectif du gouvernement fédéral de permettre de meilleurs flux de données entre les organisations au bénéfice des consommateurs, comme l'exprime le budget fédéral de 2025.

4.3 Droit au retrait (art. 54)

La LPVPDC confère aux personnes un nouveau droit de demander qu'une organisation retire leurs renseignements personnels. Le retrait signifie la suppression permanente et irréversible des renseignements personnels ou leur anonymisation. Toutefois, le droit au retrait prévu par la LPVPDC ne comprend pas de droit à la désindexation, ni de droit à l'oubli, contrairement à la Loi sur le secteur privé du Québec et au RGPD.

L'organisation doit donner suite à la demande, et ce, dès que possible, si :

- Les renseignements ont été recueillis, utilisés ou communiqués en contravention de la LPVPDC;
- La personne a retiré son consentement;
- Les renseignements ne sont plus nécessaires à la fourniture d'un produit ou d'un service demandé par la personne.

Bien que certains puissent soutenir qu'une obligation similaire existait déjà implicitement sous le régime de la LPRPDE lorsque le consentement était retiré ou que les fins initiales avaient été réalisées, la LPVPDC va plus loin. En particulier, le droit au retrait peut s'appliquer même lorsqu'une finalité plus large n'est pas nécessairement épuisée, si les renseignements ne sont plus nécessaires à la fourniture du produit ou du service demandé par la personne.

Par exemple, lorsqu'une organisation a recueilli des renseignements personnels à la fois pour fournir un service et pour des fins secondaires comme le marketing, une personne qui ne souhaite plus bénéficier du service pourrait être en mesure de demander le retrait de ces renseignements, même si l'organisation avait auparavant l'opportunité de soutenir, sous le régime de la LPRPDE, qu'elle pouvait les conserver pour d'autres fins consignées.

Fait important, si les renseignements personnels visés par la demande ont été transférés à un fournisseur de services, la LPVPDC exige que l'organisation l'en informe dès que possible et qu'elle veille à ce que le retrait soit effectué. Cette exigence sera lourde et difficile à mettre en œuvre pour les organisations qui font affaire avec de nombreux fournisseurs de services.

Pour les deux derniers motifs seulement, soit le retrait du consentement et le fait que les renseignements ne sont plus nécessaires, l'organisation peut refuser si :

- Les renseignements ne peuvent être séparés des renseignements personnels d'une autre personne sans fardeau excessif;
- Une autre loi ou un contrat empêche le retrait;
- Les renseignements sont nécessaires à une défense ou à un recours juridique;
- Le retrait nuirait à l'exactitude ou à l'intégrité de renseignements nécessaires à la fourniture continue d'un produit ou d'un service, lorsque les renseignements ne concernent pas un enfant;
- La demande est vexatoire ou faite de mauvaise foi;
- L'effet négatif du retrait sur l'organisation l'emporte sur l'effet négatif de la conservation sur la personne.

Tout refus doit être expliqué par écrit, y compris les recours dont dispose la personne pour le contester sous le régime de la LPVPDC. Si le refus est fondé sur le motif de « l'effet négatif sur l'organisation », il doit également être déclaré à la Commission. Par ailleurs, si les données ont été communiquées à un fournisseur de services, l'organisation doit s'assurer que celui-ci les retire également.

Réserve : renseignements dépersonnalisés et droits individuels

La LPVPDC exclut les renseignements personnels dépersonnalisés des droits d'accès et de rectification, de mobilité des données et de retrait, une exclusion qui semble reconnaître le fardeau commercial auquel l'organisation serait autrement confrontée si elle devait réidentifier les renseignements pour se conformer à ces droits. En pratique, cela crée une forte incitation pour l'organisation à dépersonnaliser les renseignements personnels avant de les utiliser à des fins de recherche et de développement, plutôt que de chercher à obtenir le consentement pour utiliser les renseignements dans leur état initial.

5. Intelligence artificielle et systèmes décisionnels automatisés

En introduisant des dispositions sur la dépersonnalisation et l'anonymisation, la LPVPDC établit des règles attendues depuis longtemps et adaptées à l'ère actuelle de l'intelligence artificielle. Les récents signaux en matière de politique fédérale, notamment la stratégie IA pour tous du gouvernement, indiquent clairement que le Canada entend traiter de nombreux risques liés à l'IA, notamment ceux touchant l'équité, la sûreté, l'intégrité démocratique, les hypertrucages, les biais algorithmiques, les préjudices en ligne et l'utilisation abusive de renseignements personnels, au moyen d'une approche axée d'abord sur la sécurité et fondée sur le droit. Dans ce contexte, les dispositions de la LPVPDC relatives à l'IA s'inscrivent dans la continuité d'une orientation stratégique plus large : utiliser le droit de la protection des renseignements personnels et des données comme principal instrument de gouvernance du développement et du déploiement des systèmes d'IA, notamment en renforçant les mesures de protection contre les utilisations inappropriées de renseignements personnels et les pratiques émergentes, comme la tarification fondée sur la surveillance.

La LPVPDC clarifie enfin la distinction entre « anonymiser » et « dépersonnaliser », ce qui favorise une plus grande prévisibilité. De plus, la LPVPDC permet à l'organisation de dépersonnaliser ou d'anonymiser des renseignements personnels à l'insu de la personne et sans son consentement, réglant ainsi une ambiguïté de longue date sous le régime de la LPRPDE.

5.1 Anonymisation (art. 2(1), 6(5), 20, 54)

Sous le régime de la LPVPDC, « anonymiser » signifie modifier de façon irréversible et permanente des renseignements personnels, de sorte qu'il n'existe aucun « risque raisonnablement prévisible » qu'une personne puisse être identifiée directement ou indirectement à partir de ceux-ci. La LPVPDC ne s'applique pas aux renseignements personnels anonymisés et l'anonymisation est également considérée comme une forme de retrait.

L'inclusion d'une norme de raisonnabilité dans l'évaluation du risque de réidentification est également conforme au régime québécois d'anonymisation (voir l'article 23 de la Loi sur le secteur privé et le *Règlement sur l'anonymisation des renseignements personnels*), qui encadre lui aussi l'anonymisation en fonction du caractère raisonnablement prévisible du risque de réidentification.

Pour les organisations, un cadre juridique clair encadrant l'utilisation de renseignements anonymisés est important pour soutenir l'innovation, le développement de produits et l'entraînement de modèles d'IA, tout en offrant une plus grande certitude quant au moment où les renseignements cessent de relever du champ d'application de la LPVPDC. La Loi prévoit donc que l'anonymisation des renseignements personnels peut être assujettie à des règlements prescrits (art. 139(1)a) LPVPDC).

Aucun consentement requis. Bien que la définition de l'anonymisation confirme qu'elle implique la modification de renseignements personnels, l'article 20 de la LPVPDC précise que les organisations peuvent « utiliser » des renseignements personnels et leur appliquer des techniques d'anonymisation à l'insu de la personne et sans son consentement.

Cela est important en pratique : les organisations n'ont pas à prévoir les utilisations liées à l'anonymisation au moment de la collecte ni à inclure ces fins dans leurs avis de confidentialité, ce qui leur offre une souplesse importante pour tirer parti des données à des fins secondaires comme l'analytique, la recherche ou l'amélioration de produits, une fois celles-ci dûment anonymisées.

Bien que le droit québécois ne contienne pas de disposition explicite équivalente, la même conclusion devrait généralement s'appliquer sous le régime du *Règlement sur l'anonymisation des renseignements personnels* du Québec, puisque les renseignements anonymisés conformément à la norme applicable ne devraient plus être traités comme des renseignements personnels et ne devraient donc pas déclencher d'exigences de consentement.

5.2 Dépersonnalisation (art. 2(1), 2(2), 20 à 22, 54(3))

« Dépersonnaliser » signifie modifier des renseignements personnels de sorte qu'une personne ne puisse pas être identifiée directement à partir de ceux-ci, bien qu'un risque d'identification demeure. Contrairement aux renseignements anonymisés, les renseignements dépersonnalisés ne cessent pas d'être des renseignements personnels. Toutefois, ils sont exemptés des obligations de retrait prévues par la LPVPDC, ainsi que des obligations relatives à l'accès et à la rectification.

La LPVPDC établit des règles relatives au traitement des renseignements personnels dépersonnalisés et crée des exceptions particulières permettant leur utilisation ou leur communication sans le consentement de la personne. Cela permet à l'organisation de bénéficier d'une plus grande souplesse dans le traitement de ces renseignements dépersonnalisés.

Traitement des renseignements dépersonnalisés (art. 74 et 75, 145). Le seuil relativement peu exigeant retenu pour la dépersonnalisation, soit la suppression des renseignements permettant l'identification directe, permet à l'organisation de préserver la richesse des données au niveau des dossiers, essentielle à la recherche interne. Toutefois, la LPVPDC impose des obligations particulières lors du traitement de renseignements dépersonnalisés : l'organisation doit tenir compte du risque d'identification d'une personne lorsqu'elle applique des mesures techniques et administratives et veiller à ce que ces mesures soient proportionnelles à la finalité et à la sensibilité de ces renseignements.

La LPVPDC interdit à l'organisation d'utiliser des renseignements personnels dépersonnalisés, seuls ou combinés à d'autres renseignements, afin d'identifier une personne, sauf dans les cas suivants :

- Pour mettre à l'essai les mesures de sécurité ou les processus de dépersonnalisation qu'elle a mis en place;
- Lorsque les renseignements personnels ont été dépersonnalisés uniquement pour les protéger ou les anonymiser;
- Avec le consentement valide de la personne;
- Pour mettre à l'essai l'équité et l'exactitude des modèles, des processus et des systèmes développés à l'aide de renseignements personnels dépersonnalisés;
- Pour se conformer à la LPVPDC ou à une autre loi fédérale ou provinciale;
- Avec l'autorisation de la Division de la protection de la vie privée et des données des consommateurs, ou dans toute autre circonstance prévue par règlement;
- Lorsqu'une autre disposition de la LPVPDC s'applique.

Sous le régime de la LPVPDC, l'organisation qui contrevient sciemment à cette interdiction serait passible d'une amende pouvant atteindre le plus élevé de 25 000 000 $ ou 5 % du revenu mondial brut de l'organisation. Ensemble, l'interdiction et cette sanction reconnaissent implicitement le risque inhérent de réidentification associé aux données dépersonnalisées et visent à concilier leur utilisation avec les mesures de protection et les restrictions nécessaires pour réduire ce risque au minimum.

Exceptions au consentement pour les renseignements dépersonnalisés (art. 21 et 22). La LPVPDC permet à l'organisation d'utiliser et, dans certains cas, de communiquer des renseignements personnels à l'insu de la personne et sans son consentement s'ils sont dépersonnalisés, notamment :

- À des fins internes de recherche, d'analyse et de développement, pourvu que les renseignements soient dépersonnalisés avant leur utilisation;
- Entre les parties à une transaction commerciale éventuelle, pourvu que les renseignements soient dépersonnalisés avant leur utilisation ou leur communication et le demeurent jusqu'à la conclusion de la transaction.

La LPVPDC permet ainsi à l'organisation de réutiliser des renseignements recueillis à une fin donnée à des fins secondaires de recherche, comme l'analytique d'entreprise ou d'affaires. La disposition d'interdiction relative aux renseignements dépersonnalisés confirme également ce qui avait été anticipé à l'égard de l'apprentissage automatique : l'utilisation de renseignements dépersonnalisés pour entraîner des systèmes d'apprentissage automatique relèverait vraisemblablement aussi de l'exception relative à la « recherche et au développement ».

Exception — réidentification (art. 75). La LPVPDC crée une exception à l'interdiction générale de réidentifier des personnes à l'aide de renseignements personnels dépersonnalisés, permettant à l'organisation de mettre à l'essai l'équité et l'exactitude des modèles et des systèmes développés à l'aide de renseignements dépersonnalisés. La référence aux « modèles » vise presque certainement le résultat d'un processus d'apprentissage automatique : le résultat entraîné est couramment appelé un « modèle » dans la littérature sur l'IA.

Par conséquent, l'organisation qui met à l'essai des modèles d'apprentissage automatique afin d'en vérifier l'équité, l'exactitude ou les biais ne serait pas limitée par les restrictions relatives à la réidentification, même lorsque les données d'entraînement sous-jacentes ont été dépersonnalisées.

5.3 Systèmes décisionnels automatisés

Sous le régime de la LPVPDC, un « système décisionnel automatisé » s'entend de toute technologie qui assiste ou remplace le jugement humain dans la prise de décisions, y compris les systèmes fondés sur des règles, l'analyse de régression, l'analytique prédictive, l'apprentissage automatique, l'apprentissage profond, les réseaux neuronaux ou d'autres techniques.

La définition proposée de « système décisionnel automatisé » est volontairement large et neutre sur le plan technologique. Elle vise non seulement les outils fondés sur l'IA, mais aussi les systèmes plus traditionnels fondés sur des règles, largement utilisés par les organisations. Fait important, la définition ne se limite pas aux technologies qui remplacent entièrement la prise de décision humaine. Elle s'étend également aux systèmes qui appuient ou éclairent simplement le jugement humain.

En pratique, et par comparaison avec l'article 12.1 de la Loi sur le secteur privé du Québec, qui ne s'applique qu'aux décisions fondées exclusivement sur un traitement automatisé, cela élargit considérablement la portée des systèmes visés, puisque de nombreux outils opérationnels sont conçus pour structurer, orienter ou influencer des décisions plutôt que pour les automatiser entièrement. Sous le régime de la LPVPDC, la définition de renseignement personnel vise expressément les renseignements inférés au sujet d'une personne, ce qui s'étend aux inférences générées par l'IA.

Ouverture et transparence (art. 62). L'organisation qui utilise un système décisionnel automatisé doit rendre facilement accessible, dans un langage clair, une explication générale de la façon dont le système est utilisé pour faire des prédictions, des recommandations ou des décisions au sujet de personnes lorsque celles-ci pourraient avoir un effet juridique ou un effet tout aussi important sur elles.

Bien que l'expression « effet juridique ou effet tout aussi important » ne soit ni définie ni expliquée, les effets juridiques pourraient, en pratique, être interprétés comme des décisions ayant une incidence sur les droits et obligations d'une personne. Quant à l'« effet tout aussi important », une interprétation naturelle pourrait s'inspirer des circonstances donnant lieu à un « préjudice grave » au sens de la LPVPDC, comme une atteinte à la réputation, la perte d'un emploi, une perte financière ou des effets négatifs sur le dossier de crédit d'une personne.

Dans l'Union européenne, des orientations ont été publiées sur l'interprétation des termes « effet juridique ou effet tout aussi important ». Par exemple, la Commission Nationale de l'Informatique et des Libertés de France a indiqué qu'un tel effet signifierait que l'environnement, le comportement ou les choix d'une personne sont influencés, ou que le résultat serait discriminatoire. Pour sa part, l'Information Commissioner's Office du Royaume-Uni ne définit pas ce critère, mais donne comme exemples le « refus automatique d'une demande de crédit en ligne » et les « pratiques de recrutement électronique sans intervention humaine » comme ayant des effets tout aussi importants.

Contrairement à l'article 12.1 de la Loi sur le secteur privé du Québec, la LPVPDC vise non seulement les décisions, mais aussi les prédictions et les recommandations, pourvu qu'elles puissent avoir un effet juridique ou un effet tout aussi important sur la personne. Pour les organisations, l'inclusion de ce seuil constitue une limite bienvenue et semble empruntée à l'article 22 du RGPD[7], qui vise une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques concernant la personne concernée ou l'affectant de manière tout aussi importante.

Cette portée crée un défi opérationnel important : les organisations devront identifier et inventorier tous les systèmes visés, ce qui pourrait s'avérer complexe en pratique. De nombreux outils ayant une fonction d'orientation de la décision sont intégrés aux processus d'affaires et ne sont pas toujours formellement classés comme des « systèmes décisionnels automatisés », ce qui exigera un exercice de cartographie plus granulaire et interfonctionnel.

Droit d'être informé de la prise de décision automatisée (art. 63(5)). La LPVPDC accorde aux personnes un nouveau droit de demander une explication des décisions, des recommandations ou des prédictions automatisées qui pourraient avoir un effet juridique ou un effet tout aussi important sur elles. Ce droit se reflète dans le RGPD, mais n'a pas d'équivalent sous le régime de la LPRPDE. Sur demande, l'organisation doit expliquer :

- Les renseignements personnels utilisés;
- La source de ces renseignements;
- Les principales raisons du résultat.

Les personnes doivent également avoir la possibilité de présenter des observations écrites à un employé capable d'examiner le résultat, et les organisations doivent aider les personnes qui auraient besoin d'assistance pour préparer ces observations écrites.

Le contenu de l'explication, bien que similaire, va plus loin que l'article 12.1 de la Loi sur le secteur privé du Québec, puisqu'il exige d'indiquer les sources des renseignements. Contrairement au RGPD, toutefois, la LPVPDC n'accorde pas aux personnes le droit de s'opposer à l'utilisation de la prise de décision automatisée. De plus, il n'est pas clair si le droit de rectification s'étend aux conclusions tirées par un système décisionnel automatisé.

---

7 Voir l'article 22 du RGPD : « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. »

6. Enfants

La LPVPDC introduit une définition explicite du terme « enfant », qui remplace ainsi l'emploi généralement privilégié du terme « mineur ». La Loi définit l'« enfant » comme une personne âgée de moins de 18 ans.

L'une des caractéristiques importantes de la LPVPDC est que les renseignements personnels concernant les enfants sont réputés être sensibles. Cela est important, puisque la sensibilité ne se limite pas à une seule disposition de la Loi : elle constitue un facteur récurrent qui informe les obligations de l'organisation tout au long du cycle de vie des renseignements personnels. Par conséquent, toute organisation qui recueille, utilise ou communique des renseignements personnels d'enfants devrait évaluer avec une prudence accrue si ses pratiques sont appropriées dans les circonstances.

Consentement (art. 15(5)). La sensibilité des renseignements personnels des enfants est pertinente aux fins du consentement. Comme la sensibilité est l'un des facteurs utilisés pour déterminer si le consentement implicite est approprié, les organisations devront souvent obtenir un consentement exprès lorsqu'elles recueillent et traitent des renseignements concernant des enfants.

Fins appropriées (art. 12(2)). Comme le critère de la personne raisonnable exige expressément de tenir compte de la sensibilité des renseignements, les organisations qui recueillent, utilisent ou communiquent des renseignements d'enfants devraient évaluer soigneusement si les fins et la manière de recueillir, d'utiliser ou de communiquer ces renseignements sont appropriées.

Dépersonnalisation (art. 74). La LPVPDC exige que les organisations tiennent compte à la fois de la finalité et de la sensibilité des renseignements lorsqu'elles appliquent des mesures techniques et administratives aux renseignements dépersonnalisés. Lorsque des données concernant des enfants sont en cause, les organisations devraient donc envisager des techniques de dépersonnalisation plus robustes, des limites d'accès plus strictes et des contrôles supplémentaires afin de réduire le risque de réidentification ou d'utilisation secondaire inappropriée.

Cybersécurité et réponse aux incidents (art. 56 et 58). L'obligation de la LPVPDC relative aux mesures de sécurité est proportionnelle à la sensibilité des renseignements, ce qui signifie que les organisations qui traitent des renseignements personnels d'enfants devraient évaluer si des mesures administratives, techniques et organisationnelles supplémentaires sont requises, notamment des contrôles d'accès, des mesures d'authentification, de la surveillance, de la formation du personnel et des contrôles visant les fournisseurs de services. De plus, les renseignements personnels d'enfants seront également pertinents pour déterminer si une atteinte crée un risque réel de préjudice grave.

Conservation et retrait (art. 52 et 54(2)). Puisque la LPVPDC exige que les organisations tiennent compte de la sensibilité des renseignements lorsqu'elles déterminent les périodes de conservation, les renseignements personnels d'enfants devraient généralement être assujettis à des périodes de conservation plus courtes, avec une justification appropriée et soigneuse lorsque des périodes plus longues sont nécessaires.

L'exception permettant à une organisation de refuser une demande de retrait au motif que le retrait aurait un effet négatif indu sur l'exactitude ou l'intégrité des renseignements nécessaires à la fourniture continue d'un produit ou d'un service à la personne ne s'applique pas lorsque la demande concerne les renseignements personnels d'un enfant.

Représentants autorisés (art. 4). Les droits prévus par la LPVPDC peuvent être exercés au nom d'un enfant par un parent, un gardien ou un tuteur, sauf si l'enfant (i) souhaite exercer personnellement ces droits et (ii) est capable de le faire. Contrairement à la Loi sur le secteur privé du Québec (où l'âge pertinent est de 14 ans) ou au RGPD (où il est de 13 ans), il n'existe pas de limite d'âge précise pour exercer les droits en matière de protection des renseignements personnels, y compris le droit de recours.

7. Impartition et transferts transfrontaliers

La LPVPDC ne modifie pas de manière importante les exigences relatives à l'impartition ou aux transferts transfrontaliers. Elle intègre plutôt formellement les exigences et les pratiques exemplaires existantes et précise les obligations respectives de l'organisation qui contrôle les renseignements personnels tout comme de ses fournisseurs de services. Elle confirme également les obligations des fournisseurs de services qui utilisent des renseignements personnels à leurs propres fins. Pour les organisations, ces changements devraient apporter davantage de clarté et de cohérence.

7.1 Impartition

La LPVPDC précise la manière dont les renseignements personnels peuvent être transférés à un fournisseur de services, défini comme étant « [t]oute 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 ».

Cette définition confirme que les entités d'un même groupe d'organisations sont incluses comme fournisseurs de services. Il convient de noter que les termes « service au nom ou pour le compte d'une autre organisation » semblent avoir une portée large et ne sont pas définis davantage.

De plus, la LPVPDC introduit de nouvelles exigences pour l'organisation qui communique ou transfère des renseignements personnels à l'extérieur du Canada.

Obligations de l'organisation (art. 7, 11, 19, 54 et 56). Sous le régime de la LPVPDC, l'organisation peut transférer les renseignements personnels d'une personne à un fournisseur de services à son insu et sans son consentement. La Loi sur le secteur privé du Québec contient une disposition équivalente à l'article 18.3.

Selon l'article 7 de la LPVPDC, les renseignements personnels recueillis, utilisés ou communiqués par un fournisseur de services pour le compte de l'organisation demeurent sous le contrôle de l'organisation, et non du fournisseur de services, tant que l'organisation décide de recueillir les renseignements et détermine les fins de leur collecte, de leur utilisation ou de leur communication.

The organization must:

- Veiller, par contrat ou autrement, à ce que le fournisseur de services assure aux renseignements un niveau de protection équivalent à celui que l'organisation elle-même doit fournir sous le régime de la LPVPDC;
- Établir ses mesures de sécurité et tenir compte de toute incidence raisonnablement prévisible sur la vie privée pouvant découler du transfert de renseignements personnels à un fournisseur de services;
- Aviser tout fournisseur de services auquel des renseignements personnels ont été transférés dès que possible après avoir retiré ces renseignements à la demande d'une personne et veiller à ce que le fournisseur de services les retire également.

En pratique, cela signifie que l'organisation devrait conclure une entente de partage de renseignements personnels avant de transférer les renseignements à un tiers.

Obligations des fournisseurs de services (art. 11, 19, 54(5), 56(2), 61 et 71(3)). Contrairement à la LPRPDE, la LPVPDC impose expressément des obligations aux fournisseurs de services. Ceux-ci doivent établir des mesures de sécurité appropriées et aviser l'organisation dès que possible en cas d'atteinte

aux mesures de sécurité. Les organisations qui contrôlent les renseignements personnels sont ensuite responsables d'aviser les personnes et la Commission. De plus, les fournisseurs de services doivent être en mesure d'exécuter une demande de rectification ou de retrait présentée à l'organisation qui contrôle les renseignements.

En revanche, la Loi sur le secteur privé du Québec ne contient pas de disposition équivalente imposant expressément des obligations relatives aux mesures de sécurité et à l'avis en cas d'atteinte directement aux fournisseurs de services. L'organisation demeure plutôt responsable des mesures de sécurité raisonnables et de l'avis en cas d'atteinte en vertu des articles 10 et 3.5, tandis que l'article 18.3 exige que les ententes de partage de renseignements personnels comprennent des protections en matière de confidentialité et des restrictions relatives à l'utilisation. En pratique, les obligations des fournisseurs de services en matière de sécurité et d'avis en cas d'incident sont donc traitées contractuellement.

Bien que la LPVPDC impose plus clairement des obligations particulières à chaque partie, nous recommandons tout de même aux organisations d'établir les rôles et les responsabilités en cas d'atteinte dans une entente de partage de renseignements personnels.

Même si un fournisseur de services n'est par ailleurs pas assujetti à la partie 1 de la LPVPDC à l'égard des renseignements qu'il traite pour le compte d'une autre organisation, il devient assujetti à toutes ces obligations s'il recueille, utilise ou communique des renseignements personnels transférés par une autre organisation à toute fin autre que celle pour laquelle ils lui ont été transférés.

7.2 Transferts transfrontaliers (art. 6, 57 et 62)

La LPVPDC s'applique aux renseignements personnels que l'organisation recueille, utilise ou communique à l'échelle interprovinciale ou internationale. Avant de communiquer ou de transférer des renseignements personnels à l'extérieur du Canada, une organisation doit :

- Réaliser une EFVP et fournir à la Commission l'accès à celle-ci, ou une copie de celle-ci, sur demande;
- Mettre en œuvre des mesures pour atténuer les risques relevés dans l'EFVP, comme des mesures contractuelles de protection des renseignements personnels, l'adhésion à un code de pratique ou un processus de certification approuvé par la Division de la protection de la vie privée et des données des consommateurs;
- Indiquer si elle transfère ou communique des renseignements personnels à l'échelle interprovinciale ou internationale d'une manière susceptible d'avoir des incidences raisonnablement prévisibles sur la vie privée.

La nouvelle exigence d'EFVP applicable aux transferts transfrontaliers rapproche la LPVPDC du cadre québécois, où l'article 17 de la Loi sur le secteur privé exige la réalisation d'une évaluation des facteurs relatifs à la vie privée avant la communication de renseignements personnels à l'extérieur du Québec. En pratique, la LPVPDC formalise une exigence qui était déjà largement reconnue comme une pratique exemplaire pour les transferts internationaux.

Elle peut également être interprétée comme s'inscrivant dans une préoccupation fédérale plus large à l'égard de la souveraineté des données : le pilier 4 de la stratégie IA pour tous met l'accent sur la construction d'une assise souveraine canadienne en matière d'IA et souligne que, à l'ère de l'IA, la souveraineté dépend non seulement de l'infrastructure et de la capacité de calcul, mais aussi des données qui alimentent les systèmes d'IA.

8. Mesures de sécurité et réponse aux incidents

La LPVPDC comprend une obligation relative aux mesures de sécurité très semblable à celle actuellement prévue par la LPRPDE : l'obligation de protéger les renseignements personnels au moyen de mesures de sécurité physiques, organisationnelles et technologiques « proportionnelles ». La sensibilité deviendrait le nouveau principal facteur permettant d'évaluer le caractère adéquat des mesures de sécurité, bien que « la quantité, la répartition, le format et le mode de stockage des renseignements » demeurent pertinents.

Une organisation peut évaluer si ses mesures de sécurité sont « proportionnelles » en réalisant une évaluation structurée fondée sur les risques, qui met en relation la sensibilité et le volume des renseignements personnels qu'elle détient avec la probabilité et l'incidence d'un préjudice découlant d'une atteinte, puis en comparant ses contrôles à des normes reconnues, comme le NIST CSF ou ISO 27001, à des orientations réglementaires et aux pratiques de pairs dans son secteur.

Cette démarche implique généralement de documenter les risques identifiés, de faire correspondre les mesures physiques, techniques et organisationnelles existantes à ces risques, d'en vérifier l'efficacité au moyen d'audits ou d'exercices de simulation, de repérer les lacunes lorsque les contrôles sont inférieurs aux normes du secteur pour des organisations comparables, et d'établir un plan d'atténuation.

8.1 Authentification (art. 56)

La LPVPDC élargit la portée des obligations de l'organisation en matière de mesures de sécurité. En plus de protéger les renseignements personnels contre la perte, le vol ou l'accès, la communication, la copie, l'utilisation ou la modification non autorisés, l'organisation doit également mettre en œuvre des mesures raisonnables pour authentifier l'identité de la personne à laquelle les renseignements personnels se rapportent.

Il convient de noter que cette nouvelle exigence vise uniquement l'« authentification », c'est-à-dire la vérification ou la confirmation de l'identité d'une personne, et non l'« identification », qui consiste à rechercher dans une base de données afin de déterminer qui est une personne.

La LPVPDC exige que l'organisation mette en œuvre des mesures de sécurité « raisonnables » à cette fin de vérification, plutôt que pour identifier une personne de façon absolue. À cette fin, l'organisation devrait évaluer les risques de fraude et de vol d'identité lorsqu'elle détermine les mesures de protection appropriées pour les renseignements personnels utilisés aux fins d'authentification, et devrait envisager l'adoption de pratiques exemplaires en matière de sécurité de l'information.

8.2 Avis et déclaration (art. 58, 59 et 61)

La LPVPDC maintient les exigences d'avis et de déclaration applicables aux « atteintes aux mesures de sécurité » telles qu'elles existent sous le régime de la LPRPDE, notamment en exigeant que l'organisation prenne les mesures suivantes lorsqu'une atteinte aux mesures de sécurité crée un risque réel de préjudice grave :

- Déclarer l'atteinte à la Commission;
- Aviser la personne touchée de l'atteinte dès que possible après que l'organisation a conclu que l'atteinte est survenue;
- Aviser toute autre organisation ou institution gouvernementale de l'atteinte si l'organisation estime que cela pourrait contribuer à réduire ou autrement atténuer le risque de préjudice.

La LPVPDC introduirait également une nouvelle exigence applicable aux fournisseurs de services : si un fournisseur de services conclut qu'une atteinte aux mesures de sécurité mettant en cause des renseignements personnels est survenue, il doit en aviser dès que possible l'organisation qui contrôle ces renseignements.

Cette exigence établirait un seuil minimal prévu par la loi pour l'avis donné par les fournisseurs de services, une question habituellement régie par les modalités des ententes avec ceux-ci. Le critère déclencheur de l'avis, soit la conclusion qu'une atteinte aux mesures de sécurité mettant en cause des renseignements personnels est survenue, donnerait au fournisseur de services le temps d'enquêter sur les incidents de sécurité avant de donner avis. Comme sous le régime de la LPRPDE et de la Loi sur le secteur privé du Québec, aucun délai fixe n'est prévu pour l'avis, qui doit être donné dès que possible, sans échéance déterminée comme celle prévue par le RGPD, par exemple dans les 72 heures.

9. Conservation et retrait

À l'instar du principe 5 de la LPRPDE, la LPVPDC impose à l'organisation des obligations relatives à la conservation des renseignements. Une organisation ne doit pas conserver les renseignements personnels au-delà de la période nécessaire pour :

- Réaliser les fins auxquelles ils ont été recueillis, utilisés ou communiqués;
- Se conformer à la LPVPDC, à toute autre loi fédérale ou provinciale, ou aux modalités raisonnables d'un contrat.

Une fois cette période terminée, l'organisation doit retirer les renseignements dès que possible. Les organisations devraient noter que la définition de « retirer » comprend l'anonymisation, ce qui pourrait s'avérer utile lorsque la destruction serait impraticable ou difficile.

La LPVPDC est toutefois plus prescriptive que la LPRPDE, puisqu'elle ajoute l'exigence selon laquelle l'organisation doit tenir compte de la sensibilité des renseignements lorsqu'elle fixe la période de conservation. Si les renseignements ont été utilisés pour prendre une décision au sujet d'une personne, ils doivent être conservés pendant une période suffisante pour permettre à celle-ci de présenter une demande d'accès (à titre de référence, cette période est d'un an sous le régime de la Loi sur le secteur privé du Québec). Comme sous le régime de la LPRPDE, l'organisation doit également conserver les renseignements aussi longtemps que nécessaire pour permettre à la personne d'épuiser tout recours prévu par la LPVPDC.

Prochaines étapes

Le projet de loi C-36 attend actuellement la deuxième lecture à la Chambre des communes, la première lecture ayant eu lieu le 15 juin 2026. Par la suite, le Sénat devra tenir ses trois propres lectures avant l'adoption officielle de la Loi. En juin 2026, il n'existe aucune indication claire quant à la rapidité avec laquelle le projet de loi franchira les prochaines étapes.

BLG mettra ce document à jour au fur et à mesure que le projet de loi franchira les étapes du processus législatif afin de refléter fidèlement les changements juridiques.

Auteurs :

Élisabeth Lesage-Bigras
T 514.395.2749
ELesageBigras@blg.com

Krystin Chung
T 416.367.6000
KChung@blg.com

Claire Feltrin
T 604.323.3473
CFeltrin@blg.com

Frédéric Wilson
T 514.954.2509
FWilson@blg.com

Candice Hévin
T 514.954.2588
CHevin@blg.com

Principaux contacts :

Hélène Deschamps-Marquis
T 514.954.3102
HDeschampsMarquis@blg.com

Dan Michaluk
T 416.367.6097
DMichaluk@blg.com

Frédéric Wilson
T 514.954.2509
FWilson@blg.com

Eric Charleston
T 416.367.6566
ECharleston@blg.com

Borden Ladner Gervais