Borden Ladner Gervais

Réforme des lois québécoises en matière de protection des renseignements personnels : **Guide de conformité pour les entreprises**

mis à jour : octobre 2022

Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises

Ce Guide a pour objectif d'outiller les entreprises en vue de l'entrée en vigueur des nouvelles exigences introduites à la *Loi sur la protection des renseignements personnels dans le secteur privé* (« **LPRPSP** ») suite à l'adoption du projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (« **Loi 64** »*). Le Québec est officiellement la première juridiction au Canada à mettre à jour ses lois en matière de protection des renseignements personnels suivant la tendance initiée par le *Règlement général sur la protection des données* (« **RGPD** ») de l'Union européenne.

Ce Guide est divisé en différents thèmes qui reflètent les principaux changements apportés par la Loi 64 au régime de protection des renseignements personnels dans le secteur privé. Ainsi, ce document est destiné à toute personne qui recueille, détient, utilise ou communique des renseignements personnels à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du *Code civil du Québec* (« **CCQ** ») (« **entreprise** »).

Pistes de conformité

Nous avons suggéré, pour chaque thème, certaines mesures que les entreprises peuvent envisager afin de se donner une longueur d'avance en matière de conformité et se préparer à l'entrée en vigueur des nouvelles dispositions.

Incertitudes

Considérant que plusieurs exigences introduites par la Loi 64 sont de droit nouveau, certaines dispositions soulèvent certains défis d'interprétation. Nous avons donc identifié les éléments sur lesquels les entreprises devraient porter une attention particulière à l'aide du **symbole !**.

* Cette abréviation est conforme à la coutume voulant que l'on désigne une loi par le numéro du projet de loi qui en est à l'origine (ex. Loi 101, Loi 21, Loi 96, etc.). Certains utilisent toutefois l'appellation « Loi 25 » en référence au numéro de chapitre (c. 25) de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* dans le Recueil annuel des lois du Québec de 2021, qui correspond à l'ordre de sanction de cette loi au cours de l'année 2021.

Table des matières

Entrée en vigueur

Tout d'abord, il importe de préciser le délai dont les entreprises disposent pour ajuster leurs pratiques d'ici l'entrée en vigueur de la Loi 64. Ainsi, sauf exception, les modifications apportées à la LPRPSP entreront en vigueur le **22 septembre 2023**, soit deux ans après la date de sanction de la Loi 64. Toutefois, certaines dispositions sont entrées en vigueur le 22 septembre 2022 (notamment le rôle de responsable de la protection des renseignements personnels et le signalement obligatoire des incidents de confidentialité, voir les nouveaux articles 3.1 et 3.5 à 3.8). Notons que le droit à la portabilité des données (art. 27 al. 3) est la seule disposition de la Loi 64 qui entrera en vigueur le 22 septembre 2024. Nous avons préparé le tableau suivant pour résumer la période d'entrée en vigueur des principales modifications apportées par la Loi 64 à la LPRPSP.

Article(s)	Exigence	Entrée en vigueur	Voir
3.1	Nomination d'un responsable de la protection des renseignements personnels	**Septembre 2022**	Section 2.1
3.2	Adoption de politiques et de pratiques de protection des renseignements personnels	**Septembre 2023**	Section 2.2
3.3 et 3.4	Évaluation des facteurs relatifs à la vie privée	**Septembre 2023**	Section 2.3
3.5 à 3.8	Signalement d'un incident de confidentialité	**Septembre 2022**	Section 7.2
8 à 8.2	Obligation d'information et de transparence	**Septembre 2023**	Section 3.1
8.1	Technologies d'identification, de géolocalisation et de profilage	**Septembre 2023**	Section 3.2
8.3, 12 et 14	Nouvelles exigences en matière de consentement	**Septembre 2023**	Section 3
9.1	Protection de la vie privée par défaut	**Septembre 2023**	Section 2.4
12	Exceptions au consentement pour l'utilisation de renseignements personnels	**Septembre 2023**	Section 3.3
12.1	Prise de décision automatisée	**Septembre 2023**	Section 4.3 et 5.3
17	Communication de renseignements personnels à l'extérieur du Québec	**Septembre 2023**	Section 6.2

Article(s)	Exigence	Entrée en vigueur	Voir
18.3	Communication de renseignements personnels à un fournisseur de services	**Septembre 2023**	Section 6.1
18.4	Communication de renseignements personnels dans le cadre d'une transaction commerciale	**Septembre 2022**	Section 3.3
21 à 21.0.2	Communication de renseignements personnels à des fins de recherche	**Septembre 2022**	Section 4.1
23	Conservation et destruction des renseignements personnels	**Septembre 2023**	Section 7.1
27	Droit à la portabilité des données	**Septembre 2024**	Section 5.2
28.1	Droit à l'oubli	**Septembre 2023**	Section 5.1
90.1 à 93.1	Nouveaux mécanismes de mise en œuvre	**Septembre 2023**	Section 1
44 et 45	Modifications aux dispositions de la LCCJTI en matière de biométrie	**Septembre 2022**	Section 7.3

1. Nouveaux mécanismes de mise en œuvre

En vigueur le 22 septembre 2023

La Loi 64 prévoit trois types de mécanismes afin d'assurer la conformité des entreprises aux nouvelles exigences introduites à la LPRPSP, soit (1) des sanctions administratives pécuniaires (2) des sanctions pénales et (3) un droit privé d'action.

Sanctions administratives pécuniaires (art. 90.1 à 90.17). La Loi 64 introduit un tout nouveau régime de sanctions administratives pécuniaires (« **SAP** ») administré par la Commission d'accès à l'information (« **CAI** »). En vertu de ces nouvelles dispositions, une « personne désignée par la Commission, mais qui n'est pas membre de l'une de ses sections » pourra imposer des SAPs aux entreprises qui contreviennent à la loi (voir le tableau ci-dessous pour les infractions précises) pouvant aller jusqu'à 10 000 000$ ou 2% du chiffre d'affaires mondial. À cet égard, il est pertinent de souligner que la personne chargée de l'imposition des SAPs n'a pas encore été désignée par la CAI. Ceci étant dit, la Loi 64 prévoit que la CAI doit publier un cadre général d'application des SAPs qui précisera notamment les objectifs poursuivis par le nouveau régime et les critères de détermination de la décision d'imposer une sanction et son montant (art. 90.2). Un tel cadre pourrait ressembler à celui élaboré par le Ministère de l'Environnement et de la Lutte contre les changements climatiques pour l'application du régime de SAP prévu en vertu de la législation environnementale.

Sanctions pénales (art. 91 à 93). La Loi 64 crée plusieurs nouvelles infractions à la LPRPSP (voir le tableau ci-dessous pour les infractions précises) en vertu desquelles la CAI peut intenter des poursuites pénales. Celles-ci pourront désormais être sanctionnées par l'imposition, par la Cour du Québec, d'une amende pouvant aller jusqu'à 25 000 000$ ou 4% du chiffre d'affaires mondial.

Dommages punitifs (art. 93.1). La Loi 64 reconnaît la possibilité pour les individus de réclamer des dommages-intérêts punitifs d'au moins 1 000$ lorsqu'une atteinte illicite à un droit conféré par la LPRPSP ou par les articles 35 à 40 CCQ cause un préjudice et que cette atteinte est intentionnelle ou résulte d'une faute lourde. L'article 93.1 LPRPSP, qui entrera en vigueur le 22 septembre 2023, constitue une nouvelle disposition d'attribution de dommages-intérêts punitifs au sens de l'article 1621 CCQ.

Les tableaux suivants proposent une synthèse des nouveaux mécanismes de mise en œuvre introduits par la Loi 64 dans la LPRPSP.

1.1. Infractions

	Sanction pénale	SAP	Dommages punitifs
Collecte, utilisation communication, conservation ou destruction de renseignements personnels en contravention à la LPRPSP	6	6	6
Défaut d'informer les personnes concernées conformément aux articles 7 et 8 au moment de recueillir leurs renseignements personnels		6	6
Défaut de prendre les mesures de sécurité propres à assurer la protection des renseignements personnels conformément à l'article 10	6	6	6
Défaut d'aviser la CAI ou les personnes concernées par un incident de confidentialité qui présente un risque de préjudice sérieux	6	6	6
Défaut d'informer la personne visée par une décision automatisée ou ne pas lui donner l'occasion de présenter ses observations		6	6
Procéder ou tenter de procéder à l'identification d'une personne physique à partir de renseignements dépersonnalisés ou anonymisés sans l'autorisation de la personne qui les détient	6		6
Entraver le déroulement d'une enquête, d'une inspection ou l'instruction d'une demande par la CAI	6		
Exercer des représailles ou menacer une personne de représailles pour le motif qu'elle a de bonne foi déposé une plainte à la CAI ou collaboré à une enquête	6		6
Refuser ou négliger de se conformer, dans le délai fixé, à une demande de production de documents émise par la CAI	6		
Contrevenir à une ordonnance de la CAI	6		

1.2. Aspects procéduraux

	Sanction pénale	SAP	Dommages punitifs
Délai de prescription	5 ans	2 ans	3 ans
Avis de non-conformité préalable	Optionnel*	Oui	Non
Possibilité de conclure un engagement de conformité	Non	Oui	Non
Sanction imposée par la	Cour du Québec	Personne désignée par la CAI	Cour du Québec ou Cour supérieure (selon le montant de la réclamation)
Révision administrative	Non	Oui	Non
Droit d'appel ou de contestation	Oui – Cour supérieure	Oui – Cour du Québec	Sur permission d'un juge de la Cour d'appel (si la valeur du litige est de moins de 60 000$)

* Le nouvel article 90.2 prévoit qu'un avis de non-conformité doit faire mention du fait que le manquement constaté par la CAI pourrait donner lieu à une SAP ou à une sanction pénale. Toutefois, l'obligation d'envoyer un avis de non-conformité à l'entreprise contrevenante se matérialise uniquement avant l'imposition d'une SAP (art. 90.4). Ainsi, il n'est pas certain si l'introduction d'une poursuite pénale par la CAI sera nécessairement précédée par un avis de non-conformité (et donc d'un délai pour remédier au manquement). Ceci étant dit, le nouvel article 92 précise que le recours pénal de la CAI est assujetti aux dispositions du *Code de procédure pénale*.

1.3. Sanctions

Sanction pénale	SAP	Dommages punitifs
Montant maximal de la sanction		
25 000 000$ ou 4% du chiffre d'affaires mondial de l'exercice financier précédant	10 000 000$ ou 2% du chiffre d'affaires mondial de l'exercice financier précédent	Montant des dommages-intérêts punitifs
Facteurs de détermination		
• La nature, la gravité, le caractère répétitif et la durée de l'infraction • La sensibilité des renseignements personnels concernés • Le fait que le contrevenant ait agi de façon intentionnelle ou avec négligence ou insouciance • Le caractère prévisible de l'infraction ou le défaut d'avoir donné suite aux recommandations ou aux avertissements visant à la prévenir • Les tentatives du contrevenant de dissimuler l'infraction ou son défaut de tenter d'en atténuer les conséquences • Le fait que le contrevenant ait omis de prendre des mesures raisonnables pour empêcher la perpétration de l'infraction • Le fait que le contrevenant, en commettant l'infraction ou en omettant de prendre des mesures pour l'empêcher, ait accru ses revenus ou ait réduit ses dépenses ou avait l'intention de le faire • Le nombre de personnes concernées par l'infraction et le risque de préjudice associé	• La nature, la gravité, le caractère répétitif et la durée du manquement • La sensibilité des renseignements personnels concernés • Le nombre de personnes concernées par le manquement et le risque de préjudice associé • Les mesures prises par la personne en défaut pour remédier au manquement ou en atténuer les conséquences • Le degré de collaboration offert à la CAI • La compensation offerte par la personne en défaut, à titre de dédommagement, à toute personne concernée • La capacité de payer de la personne en défaut	Selon la jurisprudence

2. Responsabilité et gouvernance

La Loi 64 reconnaît formellement que toute entreprise est responsable d'assurer la protection des renseignements personnels qu'elle détient (art. 3.1 al. 1). Il découle de ce principe plusieurs obligations en matière de responsabilité et de gouvernance des données, dont certaines sont entrées en vigueur dès septembre 2022.

2.1. Responsable de la protection des renseignements personnels

En vigueur le 22 septembre 2022

Désignation. La Loi 64 prévoit que par défaut la personne ayant la plus haute autorité au sein de l'entreprise (par ex. son PDG) doit veiller au respect de la mise en œuvre de la LPRPSP et exercer la fonction du « responsable de la protection des renseignements personnels » (art. 3.1 al. 2). Ce rôle de « **responsable de la PRP** » peut toutefois être délégué par écrit, en tout ou en partie, à toute personne (art. 3.1 al. 2), qu'il s'agisse d'une personne à l'interne ou d'un tiers. L'entreprise devra s'assurer que le titre et les coordonnées du responsable de la PRP sont accessibles sur son site Internet (art. 3.1 al. 3).

Tâches. Le responsable de la PRP devra veiller à la réalisation, au minimum, des tâches suivantes :

- Approuver les politiques et pratiques en matière de renseignements personnels que l'entreprise doit établir et mettre en œuvre (art. 3.2 al. 1). Voir la section 2.2 ci-dessous pour plus de détails sur ces politiques et pratiques.
- Participer aux évaluations des facteurs relatifs à la vie privée (« **EFVP** ») concernant certains systèmes d'information ou de prestation électronique de services (art. 3.3 al. 2) et suggérer des mesures afin d'assurer la protection des renseignements personnels traitées dans le cadre de ces systèmes (art. 3.4). Voir la section 2.3 ci-dessous pour plus de détails sur les EFVP.
- Consigner toute communication (faite sans consentement) à une entreprise ou organisme public susceptible de diminuer le préjudice causé par un incident de confidentialité (art. 3.5 al. 2) et prendre part à l'évaluation du préjudice causé par un incident de confidentialité (art. 3.7). Voir la section 7.2 pour plus de détails sur les incidents de confidentialité.
- Recevoir et répondre aux demandes d'accès et de rectification ainsi qu'aux demandes liées à la portabilité des données et au droit à l'oubli (art. 32, 34, 35). Voir la section 5 pour plus de détails sur les nouveaux droits individuels.

Qualifications. La Loi 64 ne prévoit pas explicitement que le responsable de la PRP doit être situé au Québec, avoir des connaissances particulières de la loi québécoise ou de la langue français. Une entité québécoise d'un groupe d'entreprises ayant des activités à l'international pourrait donc potentiellement déléguer le rôle du responsable de la PRP à une personne qui exerce un rôle similaire à l'échelle nationale (par ex. Canada), régionale (par ex. Amérique du Nord) ou mondiale.

Différences avec le RGPD. Il est intéressant de noter certaines différences entre le rôle de responsable de la PRP et celui de délégué à la protection des données sous le RGPD (voir les articles 37 et 38 du RGPD):

- La Loi 64 n'exige pas l'allocation de ressources au responsable de la PRP.
- La Loi 64 n'interdit pas à l'entreprise de donner des instructions au responsable de la PRP.
- La Loi 64 ne prévoit pas, non plus, d'interdictions de représailles à l'endroit du responsable de la PRP (toutefois, toute personne qui dépose une plainte ou coopère à une enquête de la CAI est protégée contre les représailles).
- Une entreprise n'est pas tenue de communiquer les coordonnées du responsable de la PRP à la CAI (bien que la CAI ait des pouvoirs étendus pour demander ces informations; ces informations doivent également être publiées sur le site Internet de l'entreprise).

Pistes de conformité

1. **Déterminer les qualifications requises pour exercer le rôle de responsable de la PRP.** Les entreprises devraient déterminer si elles possèdent l'expertise nécessaire à l'interne, si elles souhaitent recruter une personne pour exercer ce rôle ou si elles souhaitent externaliser ce rôle.
2. **Établir une description des rôles et responsabilités du responsable de la PRP.** Cette description devrait tenir compte des obligations de la Loi 64 et de la réalité de l'entreprise.
3. **Désigner par écrit une personne à titre de responsable de la PRP.** Prévoir un programme de formation pour le responsable de la PRP.
4. **Publier les coordonnées du responsable de la PRP sur le site Internet de l'entreprise.**

2.2. Politiques en matière de gouvernance et de protection des renseignements personnels

En vigueur le 22 septembre 2023

La Loi 64 reconnaît formellement le devoir des entreprises d'établir et de mettre en œuvre des politiques et des pratiques en matière de gouvernance et de protection des renseignements personnels (art. 3.2 al. 1). Celles-ci devront notamment prévoir l'encadrement applicable à :

- la conservation et la destruction des renseignements personnels;
- les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels; et
- un processus de traitement des plaintes relatives à la protection des renseignements personnels.

En outre, les entreprises seront tenues de publier des « informations détaillées au sujet de ces politiques et de ces pratiques » sur leur site Internet en termes simples et clairs (art. 3.2 al. 2). Il s'agit d'une obligation unique à l'échelle nationale et le niveau de détail qui sera requis n'est pas défini. Rien ne semble interdire que cette information soit insérée dans la politique de confidentialité de l'entreprise.

Les entreprises pourraient envisager d'intégrer cette information dans une nouvelle section de leur site Internet dédiée à la protection des renseignements personnels. De plus en plus d'entreprises créent d'ailleurs ce type de section (par ex. un « Centre de protection des renseignements personnels ») regroupant toute l'information pertinente sur le programme de protection des renseignements personnels de l'entreprise. Ceci peut inclure, notamment, un engagement envers la protection des renseignements personnels, une politique de confidentialité, une foire aux questions sur la vie privée, ainsi que des renseignements sur les certifications de sécurité de l'entreprise (ex. ISO 27001 ou SOC 2, etc.).

Pistes de conformité

1. **Effectuer un inventaire des politiques, directives, pratiques et procédures en place relativement à la protection des renseignements personnels tout au long de leur cycle de vie.**
2. **Effectuer un exercice de cartographie des données afin de documenter les pratiques de l'entreprise en matière de gestion des renseignements personnels.** Cet exercice sera utile au développement de politiques ci-dessous.
3. **Mettre à jour ou établir les politiques et procédures suivantes, lesquelles doivent établir les rôles et responsabilités des employés de l'entreprise tout au long du cycle de vie des renseignements. Les entreprises devraient mettre en œuvre les politiques suivantes (ou les intégrer dans un « cadre interne relatif à la gestion des renseignements personnels ») :**
    - Politique établissant les principes généraux relatifs à la collecte, l'utilisation et la communication de renseignements personnels.
    - Politique de conservation des données et calendrier de conservation.
    - Procédure relative aux méthodes de destruction des renseignements personnels et d'anonymisation, le cas échéant.
    - Politique et procédures relatives à la réception et le traitement de plaintes et de demandes d'individus souhaitant exercer leurs droits.
    - Politiques et procédures relatives à la sécurité des données.
    - Politique de gestion des incidents de confidentialité et plan de réponse aux incidents.

→ Suite à la page suivante

Pistes de conformité

- Politiques particulières en fonction des activités de l'entreprise, par exemple : politique sur l'utilisation des caméras de surveillance, politique sur l'utilisation de systèmes biométriques, politique sur l'utilisation de renseignements personnels pour la recherche et l'intelligence artificielle, etc.

4. **Développer un programme de formation sur les règles relatives à la protection des renseignements personnels pour les employés qui gèrent ou ont accès à des renseignements personnels.**
5. **Faire approuver les politiques et pratiques par le responsable de la PRP.**
6. **Publier de l'information détaillée au sujet des politiques et pratiques sur le site Internet de l'entreprise (par ex., en l'insérant dans sa politique de confidentialité ou en créant une section distincte sur son site Internet).**

2.3. Évaluations des facteurs relatifs à la vie privée (EFVP)

En vigueur le 22 septembre 2023

Obligation d'effectuer une EFVP. Les entreprises devront désormais procéder à une EFVP pour tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels (art. 3.3 al. 1).

Exemples de projets visés par l'obligation. La CAI a publié un *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée*, mis à jour en mars 2021. Ce guide ne reflète pas explicitement les exigences de la Loi 64. D'ailleurs, la CAI note qu'il sera revu à la lumière de la Loi 64 et qu'il pourrait être remanié en profondeur. Dans ce guide, la CAI recommande d'effectuer une EVFP pour tout projet impliquant des renseignements personnels. Bien que cela constitue un critère beaucoup plus large que celui prévu par la Loi 64, il est tout de même intéressant de noter le type de projets que cela peut inclure selon la CAI :

- Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service;
- Chercher une nouvelle clientèle, explorer de nouveaux marchés;
- Faire appel à un système d'algorithme ou d'intelligence artificielle;
- Installer un système de vidéosurveillance;
- Comparer différentes versions de bases de données ou de fichiers;
- Acquérir ou fusionner des organisations;
- Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc.

Pas de portée rétroactive. L'obligation de procéder à une EFVP n'a pas de portée rétroactive. Ainsi, les entreprises n'auront pas à évaluer les systèmes existants lors de l'entrée en vigueur du nouvel article 3.3. Toutefois, la mise à jour substantielle d'un système existant (ex. plateforme de gestion de documents) pourrait être considérée comme une « refonte » et devra donc faire l'objet d'une EFVP.

Forme et portée de l'EFVP. L'EFVP doit être « proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support » (article 3. 3 al. 4). Soulignons qu'il s'agit là des mêmes critères que ceux prévus à l'article 10 de la LPRPSP afin de qualifier les mesures de sécurité qu'une entreprise doit prendre pour assurer la protection des renseignements personnels qu'elle détient. Nous comprenons que ce critère vise à ce que l'envergure de l'EFVP soit adaptée à l'impact du projet sur la vie privée des individus. Un projet impliquant peu de renseignements personnels, et qui sont peu sensibles, ne nécessitera pas le même type d'EFVP que l'implantation d'un système biométrique visant un grand nombre d'individus, par exemple. Notons que le guide sur les EFVP de la CAI fournit des outils utiles aux entreprises qui veulent se familiariser avec le processus.

Portabilité des données. En outre, les entreprises devront s'assurer que les nouveaux projets et systèmes soient en mesure d'assurer la portabilité des données, c'est-à-dire la possibilité pour les personnes concernées d'obtenir la communication de leurs renseignements personnels dans un format technologique structuré et couramment utilisé (art. 3.3 al. 3). Voir la section 5.2 pour plus de détails sur le droit à la portabilité des données.

Pistes de conformité

1. **Développer une procédure interne sur les EFVP.** La procédure devrait, notamment :
   - Définir les critères déclenchant l'obligation d'effectuer une EFVP. Par exemple, l'entreprise pourrait établir une matrice permettant d'évaluer la nécessité d'une EFVP en fonction des activités de l'entreprise.
   - Définir un processus pour s'assurer que les projets qui requièrent une EFVP soient identifiés dès le début du projet.
2. **Communiquer la procédure au sein de l'entreprise.**
   - Les entreprises peuvent désigner des responsables dans les départements susceptibles d'initier ces projets (marketing, TI, intelligence d'affaires, approvisionnement).
   - Les responsables des départements devraient informer le responsable de la PRP dès le début d'un projet nécessitant une EFVP.
3. **Développer un gabarit pour la réalisation d'une EFVP.**
   - Le gabarit devrait être dans un format facile d'utilisation de sorte que les responsables des opérations sans connaissance de pointe en matière de protection des renseignements personnels puissent effectuer une première version.
   - Former le personnel approprié sur la façon de compléter une EFVP.

2.4. Paramètres de confidentialité et protection de la vie privée par défaut

En vigueur le 22 septembre 2023

Plus haut niveau de confidentialité. La Loi 64 prévoit qu'une entreprise qui recueille des renseignements personnels en offrant au public un produit ou un service technologique disposant de paramètres de confidentialité doit s'assurer que, par défaut, ces paramètres assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée (art. 9.1 al. 1). Cette exigence ne s'applique toutefois pas aux témoins de connexions (cookies) (art. 9.1 al. 2). Selon le libellé de la disposition, nous comprenons qu'elle ne s'applique pas non plus à un produit ou service destiné aux employés d'une entreprise (intranet, applicable mobile pour employés, etc.). L'article 9.1 ne fournit aucun qualificatif permettant de déterminer ce qui sera considéré comme étant « le plus haut niveau de confidentialité » dans un contexte donné. Elle risque donc de causer des défis d'interprétation pour les entreprises.

Protection de la vie privée dès la conception. Cette exigence peut sembler s'inspirer de l'approche de « protection de la vie privée dès la conception » en vertu notamment de l'article 25 du RGPD. Cette approche vise à assurer le respect du droit à la vie privée des personnes concernées à chaque étape du processus de développement d'une initiative, et rend toutes les parties prenantes responsables de veiller à ce qu'un produit ou un service particulier protège la vie privée. L'obligation sous la Loi 64 semble toutefois avoir une portée beaucoup plus restreinte, puisqu'elle ne vise que les paramètres de confidentialité et non le cycle complet de développement d'un produit ou service.

Témoins de connexion et autres fonctions technologiques. L'interaction du nouvel article 9.1 avec l'article 8.1 (voir la section 3.2) en matière de témoins de connexion suscite une certaine confusion. Alors que le législateur a pris soin d'exclure expressément les témoins de connexion du champ d'application de l'article 9.1, il ne les a pas exclus de la portée de l'article 8.1. L'article 8.1 s'applique à la collecte de renseignements personnels par tout moyen technologique comprenant des fonctions permettant de profiler, localiser ou identifier l'individu. Dans ce cas, une entreprise doit informer les individus des moyens d'activer ces fonctions. Cela implique un geste positif de la part de l'individu pour signifier son intention d'activer une fonction spécifique. De plus, selon les débats législatifs et les commentaires émis par la CAI, cette disposition doit être interprétée comme exigeant qu'une entreprise désactive ces fonctions par défaut (voir la section 3.2).

Pistes de conformité

1. Effectuer un inventaire des produits ou services technologiques offerts au public qui recueillent des renseignements personnels et qui disposent de paramètres de confidentialité.
2. Effectuer un inventaire de toutes les technologies utilisées pour recueillir des renseignements personnels et déterminer si elles comportent des fonctions permettant de profiler, de localiser ou d'identifier un individu.
3. Déterminer si ces paramètres de confidentialité ou ces fonctions technologiques doivent être ajustés pour se conformer aux nouvelles exigences de confidentialité par défaut. Cela peut inclure l'ajustement de certains paramètres de confidentialité pour fournir le plus haut niveau de confidentialité par défaut et la mise en œuvre de nouveaux processus pour demander à l'utilisateur d'activer certaines fonctions.

3. Transparence et consentement

La Loi 64 clarifie les règles applicables en matière de transparence et de consentement dans la LPRPSP.

3.1. Transparence et obligation d'information préalable au consentement

En vigueur le 22 septembre 2023

Termes simples et clairs. Sur le plan de la transparence, les entreprises ont une obligation de fournir certaines informations en « termes simples et clairs », quel que soit le moyen utilisé pour recueillir les renseignements (art. 8 al. 4).

Obligation de transparence. Cette obligation de transparence survient lors de la collecte (et par la suite, sur demande) ou dans certains cas, uniquement sur demande et, le cas échéant, lors de l'utilisation de certaines technologies :

- **Lors de la collecte.** L'entreprise qui recueille des renseignements personnels auprès d'un individu doit, lors de la collecte et par la suite sur demande, l'informer : (i) des fins auxquelles ces renseignements sont recueillis; (ii) des moyens par lesquels les renseignements sont recueillis; (iii) des droits d'accès et de rectification prévus par la loi; (iv) de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis; et le cas échéant : (v) du nom du tiers pour qui la collecte est faite; (vi) du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins auxquelles ces renseignements sont recueillis; et (vii) de la possibilité que les renseignements soient communiqués à l'extérieur du Québec (art. 8 al. 1 et 2).
- **Sur demande.** Une entreprise doit également informer, sur demande, l'individu concerné : (i) des renseignements personnels recueillis auprès de lui; (ii) des catégories d'employés qui ont accès à ces renseignements au sein de l'entreprise; (iii) de la durée de conservation de ces renseignements; et (iv) des coordonnées du responsable de la PRP (art. 8 al. 3). Lorsqu'elle recueille des renseignements personnels auprès d'une autre entreprise, une entreprise doit, à la demande de l'individu concerné, l'informer de la source de ces renseignements (art. 7) à moins qu'il s'agisse d'un dossier d'enquête constitué en vue de prévenir, détecter ou réprimer un crime ou une infraction à la loi.
- **Technologie d'identification, de localisation et de profilage.** Une entreprise qui recueille des renseignements personnels en ayant recours à une technologie qui comprend des fonctions permettant d'identifier, de localiser ou d'effectuer le profilage d'un individu doit préalablement informer l'individu du recours à une telle technologie et des moyens offerts pour activer ces fonctions (art. 8.1 al. 1 (1) et (2)). La notion de « profilage » est englobante et s'entend de la collecte et de l'utilisation de renseignements personnels afin « d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette

personne » (art. 8.1 al. 2). Ainsi, cette nouvelle exigence peut s'appliquer à diverses technologies ainsi que dans différents contextes (par exemple, certains outils de surveillance des employés, les témoins de connexion et les technologies similaires utilisées pour la publicité ciblée, etc.).

L'interprétation de l'article 8.1 soulève des difficultés puisqu'il n'est pas clair si cette disposition constitue le simple prolongement de l'obligation de transparence prévue à l'article 8 LPRPSP ou s'il s'agit d'une restriction concrète à l'utilisation de technologies de localisation, d'identification et de profilage. S'exprimant au sujet de cette nouvelle disposition en commission parlementaire, Éric Caire, ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels, a indiqué que celle-ci avait pour conséquence d'introduire un consentement explicite (opt-in) pour la collecte de renseignements personnels au moyen de technologies ayant des fonctions d'identification, de localisation ou de profilage. De plus, la CAI sur son site Web mentionne que « ces technologies ne pourront être activées par défaut; ce sera à la personne concernée de les activer si elle le souhaite ». En d'autres termes, l'individu doit poser un geste positif pour signifier son intention d'activer une fonction spécifique. Or, le libellé de l'article 8.1 se limite plutôt à une obligation d'« informer » les individus des moyens disponibles pour activer ces fonctions, sans toutefois préciser que ces moyens doivent exister dans les faits ou que les fonctions elles-mêmes doivent être systématiquement désactivées. Dans tous les cas, à la lumière des commentaires de la CAI, il est prudent d'envisager de revoir l'utilisation de certaines technologies pour profiler, localiser ou identifier des individus et, si nécessaire, de mettre en œuvre de nouveaux processus pour demander à l'utilisateur d'activer certaines fonctions. Voir la section 2.4 pour des détails concernant les exigences de protection de la vie privée par défaut.

- **Collecte par l'entremise de moyen technologique.** Une entreprise qui recueille des renseignements personnels par un moyen technologique doit publier sur son site Internet une politique de confidentialité rédigée en termes simples et clairs et la diffuser par tout moyen propre à atteindre les individus concernés (art. 8.2). L'expression « tout moyen propre » vise vraisemblablement à encourager une entreprise à informer les individus de ses pratiques en matière de traitement des renseignements en utilisant des moyens pratiques et facilement accessibles. Une entreprise a les mêmes obligations de transparence (celles détaillées à l'art. 8.2) si sa pratique et/ou sa politique fait l'objet d'une modification. En ce qui concerne le consentement, le Commissariat à la protection de la vie privée du Canada (« **CPVP** ») a publié, il y a quelques années, des *Lignes directrices pour l'obtention d'un consentement valable*, dans lesquelles il fournit des recommandations pratiques aux entreprises, notamment mettre l'accent sur certains éléments clés, permettre aux individus de déterminer à quel point et quand ils souhaitent obtenir de l'information détaillée (c'est-à-dire des avis par couches), faire preuve d'innovation et de créativité (en envisageant de mettre en œuvre des avis « juste à temps » ou d'autres outils interactifs) et faire du consentement un processus dynamique et continu (avec des conseils sur la façon de gérer la mise à jour des politique ou avis de confidentialité).

Prise de décision automatisée. La Loi 64 introduit également des exigences de transparence pour une entreprise qui utilise des renseignements personnels pour rendre une décision fondée exclusivement sur le traitement automatisé de ces renseignements (art. 12.1). Voir les sections 4.3 et 5.3 pour les détails quant à ces exigences.

Pistes de conformité

1. **Réviser et mettre à jour les politiques de confidentialité (celle visant les clients ainsi que celle visant les employés) et les formulaires et processus d'obtention de consentement.** S'assurer que les éléments suivants sont inclus en termes simples et clairs :
   - Fins auxquelles et moyens par lesquels les renseignements personnels sont recueillis.
   - Droits d'accès, de rectification et de retrait du consentement.
   - Nom du tiers pour qui la collecte est faite (le cas échéant).
   - Catégories des fournisseurs de services (le cas échéant).
   - Transfert des renseignements à l'extérieur du Québec (le cas échéant).
2. **Développer et mettre en place un processus visant à répondre aux questions et aux demandes d'information suivantes des clients ou des employés :**
   - Nature des renseignements personnels recueillis par l'entreprise.
   - Catégories d'employés qui pourraient avoir accès aux renseignements personnels.
   - Durée de conservation applicable aux renseignements recueillis auprès de l'individu.
   - Coordonnées du responsable de la PRP.
   - Source des renseignements recueillis auprès d'une autre entreprise (sauf si les renseignements ont été recueillis dans le cadre d'une enquête visant à prévenir, détecter ou réprimer un crime ou une infraction à la loi).
3. **Faire l'inventaire des technologies utilisées pour recueillir des renseignements personnels et déterminer si elles comportent des fonctions permettant de profiler, de localiser ou d'identifier un individu.**

   Le cas échéant, pour chaque fonction :
   - Vérifier si des processus adéquats sont en place pour informer les individus, au moment de la collecte, de l'utilisation de la technologie et des moyens d'activer la fonction. Le cas échéant, envisager de mettre en place de nouveaux processus pour demander à l'utilisateur d'activer la fonction.
4. **Déterminer si des renseignements personnels (de clients ou d'employés) sont collectés par l'entremise de moyens technologiques.** Le cas échéant :
   - Faire l'inventaire de ces moyens technologiques.
   - Publier une politique de confidentialité (en termes simples et clairs) sur le site Internet de l'entreprise détaillant ces collectes par l'entremise de moyens technologiques.
   - Diffuser la politique de confidentialité par tout moyen approprié pour atteindre les individus concernés par la collecte de renseignements personnels par des moyens technologiques.
   - Mettre en place une procédure pour mettre à jour la politique de confidentialité afin de s'assurer qu'elle reflète bien les pratiques de l'entreprise et que les individus sont adéquatement informés de ces changements.

3.2. Exigences du consentement : Forme, validité et mineurs

En vigueur le 22 septembre 2023

La Loi 64 apporte certaines précisions par rapport à la forme du consentement, aux critères de validité du consentement et aux exigences relatives à l'obtention du consentement de mineurs.

Forme du consentement. Pour ce qui est de la forme du consentement, la Loi 64 reconnaît la possibilité pour une entreprise de s'appuyer sur un consentement implicite pour utiliser et communiquer des renseignements personnels conformément aux fins énoncées dans sa politique de confidentialité (art. 8.3). Ceci étant dit, la Loi 64 mentionne également qu'un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, ni communiqué à un tiers, à moins que l'individu n'y consente ou que la présente loi ne le prévoit, lequel consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible (art. 12 et 13).

Il y a une incertitude relativement à l'interprétation à donner à ces dispositions, à savoir si un consentement manifesté de façon expresse doit être obtenu pour la collecte de renseignements personnels sensibles, et ce, même si l'entreprise s'est assurée de bien décrire les fins de collecte dans sa politique de confidentialité puisqu'aucune distinction n'est faite entre renseignements personnels sensibles et non sensibles à l'article 8.3. Un renseignement sensible est défini comme un renseignement qui, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée (art. 12 al. 4 (2)).

Validité du consentement. La Loi 64 précise qu'un consentement valide doit être manifeste, libre, éclairé et être donné à des fins spécifiques et demandé à chacune de ces fins, en termes simples et clairs (art. 14 al. 1). De plus, lorsqu'une demande de consentement est effectuée par écrit, l'entreprise doit s'assurer que la demande est présentée distinctement de toute autre information communiquée à l'individu.

Cela peut interdire de regrouper la demande de consentement pour des activités de traitement spécifiées avec des informations concernant d'autres sujets, par exemple les modalités d'utilisation des services de l'entreprise. Lorsqu'un individu le requiert, l'entreprise doit lui prêter assistance afin de l'aider à comprendre la portée du consentement demandé.

Consentement de mineurs. Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur (art. 4.1 et 14 al. 2) et le consentement du mineur de 14 ans et plus peut être donné par le mineur, par le titulaire de l'autorité parentale ou alors par le tuteur.

Pistes de conformité

1. **Faire l'inventaire des renseignements personnels collectés, utilisés et communiqués par l'entreprise** (clients et employés) afin de déterminer :
   - Ceux qui sont de nature sensible.
   - Ceux relatifs à des mineurs.
   - Ceux qui sont exclus du champ d'application de la loi (c.-à-d. coordonnées d'affaires).
2. **Faire l'inventaire des formulaires de consentement** ou autres documents utilisés pour obtenir le consentement des individus concernés (clients ou employés) et les réviser afin de s'assurer que :
   - Tout consentement obtenu est manifeste, libre, et éclairé.
   - Tout consentement est donné à des fins spécifiques en termes simples et clairs.
   - Lorsque la demande de consentement est faite par écrit, elle est présentée distinctement de toute autre information communiquée à l'individu.
   - Le consentement du mineur de moins de 14 ans est obtenu par le titulaire de l'autorité parentale ou par le tuteur.
   - Le consentement du mineur de 14 ans et plus est obtenu par le mineur, le titulaire de l'autorité parentale ou alors par le tuteur.
3. **Mettre en place un processus afin de s'assurer que sur demande d'un individu** (clients ou employés) :
   - L'entreprise a une procédure en place afin de lui prêter assistance et l'aider à comprendre la portée du consentement demandé.
4. **Mettre à jour la politique de classification ou de catégorisation de l'entreprise** (ou tout autre document pertinent) afin d'y refléter :
   - Les renseignements qui sont de nature sensible et ceux relatifs à des mineurs.

3.3. Exceptions à l'exigence du consentement

En vigueur le 22 septembre 2023

sauf en ce qui concerne la communication (i) dans le contexte d'une transaction commerciale et (ii) à des fins d'étude, de recherche ou de production de statistiques (22 septembre 2022)

La Loi 64 exclut certaines informations du champ d'application de la LPRPSP et introduit également des exceptions au consentement quant à certaines utilisations ou alors à certaines communications de renseignements personnels.

Cordonnées d'affaires. La Loi 64 exclut les « renseignements personnels concernant l'exercice par l'individu d'une fonction au sein d'une entreprise » du champ d'application des sections II et III de la LPRPSP (c'est-à-dire les exigences en matière d'avis et de consentement). Cela comprend « son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail » (art. 1 al. 5). Il s'agit d'une exclusion qui est similaire à celle prévue par la *Personal Information Protection Act* (« **PIPA** ») de la Colombie-Britannique et qui va au-delà de ce que prévoit la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDÉ** ») et la *Personal Information Protection Act* (« **PIPA** ») de l'Alberta, qui se limitent à exclure ces renseignements uniquement lorsque ceux-ci sont utilisés afin d'entrer en contact avec l'individu dans le cadre de son emploi, de son entreprise ou de sa profession. Quoique cette exclusion puisse être utile à certaines entreprises qui souhaitent utiliser ce type de renseignements sans consentement, ces dernières doivent appliquer les exigences de la loi canadienne anti-pourriel qui régissent l'utilisation d'adresses courriel (incluant celles de travail) pour transmettre des messages électroniques commerciaux.

Utilisation sans consentement. En vertu de la Loi 64, un renseignement personnel peut être utilisé à des fins autres que celles pour lesquelles il a été initialement collecté, sans le consentement de l'individu concerné, dans les situations suivantes :

- **Fins d'affaires légitimes.** Lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par l'individu (art. 12 al. 2 (4)) ou encore nécessaire à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité (art. 12 al. 2 (3)).
- **Intérêt de l'individu.** Lorsque son utilisation est manifestement au bénéfice de ce dernier (art. 12 al. 2 (2)).
- **Recherche, analyse de données et IA.** Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli (art. 12 al. 2 (1)) ou que son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé (art. 12 al. 2 (5) LPRPSP). Voir la section 4.2 pour des détails au sujet de cette exception et des définitions de « fins compatibles » et de renseignement « dépersonnalisé ».

Communication sans consentement. En vertu de la Loi 64, un renseignement personnel pourra être communiqué sans le consentement de l'individu concerné, dans les situations suivantes:

- **Contexte d'impartition.** Lorsque la communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service et que des mesures de protection des renseignements personnels sont prévues (art. 18.3). Voir la section 6.1 pour plus de détails sur cette exception.
- **Recherche, analyse de données et IA.** Lorsque la communication est faite à une personne ou à un organisme qui souhaite utiliser les renseignements à des fins d'étude, de recherche ou de production de statistiques et que les mesures de protection des renseignements personnels prévues à la loi sont mises en place (art. 21 à 21.0.2). Nous notons que cette exception n'est pas assujettie à l'exigence que les renseignements soient dépersonnalisés (comme c'est le cas pour l'exception en matière d'utilisation à des fins d'étude, de recherche ou de production de statistiques internes à l'organisation) bien qu'un cadre spécifique s'applique à ces types de projets de recherche. Voir la section 4 pour des détails sur ce nouveau régime.

- **Transaction commerciale.** Lorsque la communication est nécessaire pour la conclusion d'une transaction commerciale (c.-à-d. l'aliénation ou la location d'une entreprise ou des actifs dont elle dispose, une modification de sa structure juridique par fusion ou autrement, l'obtention d'un prêt, de financement ou d'une sûreté), si une entente est conclue avec l'autre partie, stipulant que cette dernière partie s'engage : (i) à n'utiliser le renseignement qu'aux seules fins de la conclusion de la transaction commerciale; (ii) à ne pas communiquer le renseignement sans le consentement de l'individu à moins d'y être autorisée par la loi; (iii) à prendre les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement; (iv) à détruire le renseignement si la transaction commerciale n'est pas conclue ou si l'utilisation de celui-ci n'est plus nécessaire (art. 18.4). Lorsque la transaction commerciale est conclue et que l'autre partie souhaite continuer d'utiliser le renseignement ou le communiquer, cette partie peut l'utiliser ou le communiquer uniquement dans la mesure prévue par la loi. Dans un délai raisonnable après la conclusion de la transaction commerciale, l'entreprise devra aviser l'individu concerné qu'elle détient maintenant ses renseignements personnels en raison de la transaction.

Relations d'emploi. Il convient de souligner que la Loi 64 n'introduit pas d'exception au consentement pour la collecte, l'utilisation ou le partage de renseignements personnels afin d'établir, gérer ou mettre fin à une relation d'emploi. En effet, un amendement visant à introduire une exception similaire à ce que prévoit la LPRPDÉ et les PIPAs de Colombie-Britannique et de l'Alberta a malheureusement été rejeté. L'absence d'une telle exception peut créer des difficultés pour les employeurs considérant les limites du modèle du consentement dans le contexte des relations employeur/employé. Il est effectivement difficile de considérer le consentement d'un employé dans ses relations avec son employeur comme étant « libre », puisqu'un employé pourrait bien croire, à tort ou à raison, que son emploi serait compromis par un refus de consentement. En outre, si un employé refuse que son employeur collecte, utilise ou communique des renseignements personnels à des fins de pratiques administratives courantes, cela pourrait empêcher l'employeur de poursuivre ses activités et de remplir ses obligations légales.

Pistes de conformité

1. **Faire l'inventaire des utilisations pouvant faire l'objet d'une exception à l'exigence du consentement** afin de déterminer si ces dernières tombent sous l'application des exceptions suivantes:
   - Utilisation nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par l'individu concerné.
   - Utilisation nécessaire à des fins de prévention et de détection de la fraude.
   - Utilisation nécessaire à des fins ou d'évaluation et amélioration des mesures de protection et de sécurité.
   - Utilisation manifestement au bénéfice de l'individu concerné.
   - Utilisation à des fins compatibles avec celles pour lesquelles le renseignement a été recueilli.
   - Utilisation nécessaire à des fins d'étude, de recherche ou de production de statistiques (et les renseignements sont dépersonnalisés).

→ Suite à la page suivante

Pistes de conformité

2. **Faire l'inventaire des communications pouvant faire l'objet d'une exception à l'exigence du consentement** afin de déterminer si ces dernières tombent sous l'application des exceptions suivantes:
   - Nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service.
   - Communication à une personne ou à un organisme qui souhaite utiliser les renseignements à des fins d'étude, de recherche ou de production de statistiques.
3. **Réviser les politiques de confidentialité et formulaires de consentement afin de :**
   - Refléter les exceptions à l'exigence de consentement et structurer ces documents de telle sorte que les utilisations ou communications exemptes de consentement soient mieux reflétées.
4. **Mettre en place une procédure visant à gérer les communications de renseignements personnels dans un contexte de transaction d'affaires** afin de s'assurer que :
   - La transaction commerciale est visée par l'exception à l'exigence du consentement au sens de la loi.
   - Toute communication de renseignements est nécessaire pour la conclusion de la transaction commerciale visée.
   - Une entente est conclue avec l'autre partie, stipulant que cette dernière s'engage: (i) à n'utiliser le renseignement qu'aux seules fins de la conclusion de la transaction commerciale; (ii) à ne pas communiquer le renseignement sans le consentement de l'individu; (iii) à prendre les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement; (iv) à détruire le renseignement si la transaction commerciale n'est pas conclue ou si l'utilisation de celui-ci n'est plus nécessaire.
   - Lorsque la transaction commerciale est conclue, s'assurer que dans un délai raisonnable après la conclusion de la transaction commerciale, l'individu concerné est avisé de la transaction par l'entreprise qui détient dorénavant ses renseignements.

4. Recherche, analyses internes et prise de décision automatisée

La Loi 64 introduit une importante réforme du régime applicable au traitement de renseignements personnels dans une perspective de recherche, ce qui permet de mieux aligner le cadre juridique québécois avec ceux des autres juridictions canadiennes.

Les modifications introduites à la LPRPSP apportent des assouplissements majeurs au régime actuel en ce qui concerne l'utilisation de renseignements personnels à des fins de recherche interne, comme l'analyse commerciale, en permettant clairement l'utilisation de renseignements personnels « dépersonnalisés » (y compris des renseignements sensibles) au sein de l'entreprise sans obtenir de consentement.

Des obligations importantes sont également introduites en ce qui concerne les décisions prises au moyen de technologies de « traitement automatisé ». Bien que non définie par la Loi 64, cette notion semble clairement viser les algorithmes d'apprentissage automatique et autres technologies associées au domaine de l'intelligence artificielle qui sont en mesure de prendre des décisions sophistiquées sans supervision humaine.

4.1. Exception au consentement pour la communication à des fins de recherche

En vigueur le 22 septembre 2022

La Loi 64 élimine la procédure d'autorisation à des fins de recherche, longtemps critiquée pour ses difficultés pratiques et pour l'incertitude engendrée par le pouvoir discrétionnaire de la CAI en matière d'évaluation des demandes d'autorisation des communications à des fins de recherche et son pouvoir de révocation.

Les modifications à l'article 21 et l'introduction des nouveaux articles 21.0.1 et 21.0.2 de la LPRPSP remplacent la procédure actuelle par un régime qui permet aux parties souhaitant partager des renseignements personnels à des fins de recherche de procéder elles-mêmes à l'évaluation de la demande de communication. Le nouveau régime met l'accent sur la vérification diligente et la transparence, et exige seulement d'informer la CAI de l'entente intervenue entre l'entreprise divulgatrice et la personne requérante (entreprise, organisme public ou chercheur individuel), ainsi que des violations de l'entente ou des événements susceptibles de porter atteinte à la confidentialité des renseignements personnels.

Évaluations des facteurs relatifs à la vie privée (EFVP). Le nouvel article 21 prévoit que les renseignements personnels peuvent être communiqués si une évaluation des facteurs relatifs à la vie privée arrive aux conclusions suivantes : (i) les renseignements personnels sont nécessaires pour atteindre l'objectif de la recherche; (ii) il est déraisonnable d'exiger de la personne requérante qu'elle obtienne le consentement des personnes concernées; (iii) l'objectif de la recherche l'emporte, eu

égard à l'intérêt public, sur l'impact de la communication sur le droit à la vie privée des personnes concernées; (iv) les renseignements sont utilisés de manière à en assurer la confidentialité, et (v) seuls les renseignements nécessaires sont communiqués (art. 21 al. 2). Il revient à l'entreprise transmettant les renseignements personnels de compléter l'EFVP, basé notamment sur les renseignements obtenus par la partie requérante.

Les entreprises qui communiquent des renseignements personnels à des fins de recherche doivent donc être prêtes à estimer le coût d'une telle évaluation, qui nécessitera généralement la contribution du service juridique de l'entreprise ou d'un conseiller juridique externe. Le coût de réalisation d'une EFVP (réalisée par l'entreprise divulgatrice ou en collaboration avec la personne requérante) peut être important et, quelle que soit la structure de l'entente avec la personne requérante, les coûts associés à cet exercice pour l'entreprise divulgatrice doivent y être comptabilisés. L'entreprise divulguant les renseignements a cependant un pouvoir discrétionnaire de ne pas communiquer les renseignements personnels demandés, même sans compléter d'EFVP.

Les entreprises qui communiquent des renseignements personnels à des fins de recherche doivent donc être prêtes à estimer le coût d'une telle évaluation, qui nécessitera généralement la contribution du service juridique de l'entreprise ou d'un conseiller juridique externe. Le coût de réalisation d'une EFVP (réalisée par l'entreprise divulgatrice ou en collaboration avec la personne requérante) peut être important et, quelle que soit la structure de l'entente avec la personne requérante, les coûts associés à cet exercice pour l'entreprise divulgatrice doivent y être comptabilisés.

Les personnes requérantes devront probablement budgétiser une somme à titre de dédommagement qui reviendra à l'entreprise divulgatrice. Le processus d'EFVP pourrait ainsi avoir pour conséquence involontaire de rendre l'accès aux renseignements personnels plus difficile pour les plus petits projets qui sont moins bien financés. L'entreprise divulgatrice pourrait toutefois accepter d'autres formes de dédommagement comme un accès prioritaire aux résultats de recherche ou la concession à des conditions avantageuses de licences sur les droits de propriété intellectuelle découlant de la recherche.

Obligations des requérants. Pour sa part, la personne requérante doit formuler sa demande par écrit et fournir à l'entreprise divulgatrice toute l'information utile au soutien de sa demande, à savoir une présentation détaillée des activités de recherche, les arguments à l'effet que les critères de l'EFVP requis par l'article 21 sont remplis, la liste des personnes et organismes à qui des demandes similaires sont faites ainsi que, le cas échéant, la description des technologies qui seront utilisées pour le traitement des renseignements (si applicable), et la décision documentée d'un comité d'éthique de la recherche relative à cette recherche (si applicable) (article 21.0.1).

Dans le cadre de ses efforts de vérification diligente préalable à la communication des renseignements, l'entreprise divulgatrice doit s'assurer que la personne requérante lui a fourni toute l'information et la documentation énoncées à l'article 21.01. Si la personne requérante est victime d'un incident de confidentialité compromettant les renseignements communiqués (voir la section 7.2), l'entreprise divulgatrice pourrait faire l'objet d'un examen minutieux advenant une enquête de la CAI.

Dispositions obligatoires de l'entente. Les deux parties à la communication de renseignements personnels à des fins de recherche doivent conclure une entente stipulant notamment que ceux-ci :

- ne peuvent être rendus accessibles qu'aux personnes à qui ont besoin d'y avoir accès dans le cadre de leurs fonctions et s'ils ont signé un engagement de confidentialité;
- ne peuvent être utilisés à des fins différentes de celles prévues à la présentation détaillée des activités de recherche;
- ne peuvent être appariés avec tout autre fichier de renseignements non prévu dans la présentation détaillée des activités de recherche;
- ne peuvent être communiqués, publiés ou autrement diffusés sous une forme permettant d'identifier les personnes concernées.

Cette entente doit également prévoir :

- les informations devant être communiquées aux personnes concernées lorsque des renseignements personnels les concernant sont utilisés pour les rejoindre en vue de leur participation à l'étude ou à la recherche;
- des mesures pour assurer la protection des renseignements;
- un délai de conservation des renseignements;
- l'obligation d'aviser la personne qui communique les renseignements de la destruction de ceux-ci;
- que la personne qui communique les renseignements et la CAI doivent être avisées sans délai : (i) du non-respect de toute condition prévue à l'entente; (ii) de tout manquement aux mesures de protection prévues à l'entente; (iii) de tout événement susceptible de porter atteinte à la confidentialité des renseignements (article 21.0.2).

Présentation de l'entente à la CAI. L'entente devra être transmise à la CAI et entrera en vigueur 30 jours après sa réception par celle-ci. Bien que les dispositions de l'article 21.0.2 n'accordent pas à la CAI le pouvoir de résilier l'entente si celle-ci ne remplit pas toutes les exigences, la CAI pourrait ordonner à l'entreprise divulgatrice de ne pas communiquer les renseignements jusqu'à ce que l'entente soit révisée pour inclure les éléments requis, suspendre l'entente ou exercer ses autres pouvoirs de surveillance prévu dans la loi. La CAI peut communiquer avec les parties pendant ou après le délai de 30 jours.

Pistes de conformité

1. Mettre en place une procédure pour les projets de recherche, afin de prévoir :

- que l'entreprise divulgatrice recevra toute la documentation énoncée à l'article 21.0.1 avant de procéder à la communication.

→ Suite à la page suivante

Pistes de conformité

- que l'entreprise verra à réaliser une évaluation des facteurs relatifs à la vie privée (EFVP), avant de procéder à la communication des renseignements et évaluer le coût de cette évaluation et envisager comment ces coûts, y compris ceux de la vérification diligente, devraient être répartis entre les parties.
- la conclusion d'une entente qui répond aux exigences de l'article 21.0.2.

2. **Remettre une copie de cette entente à la CAI au moins 30 jours avant la communication des renseignements.**

4.2. Exception au consentement pour la recherche et les analyses internes

En vigueur le 22 septembre 2023

La Loi 64 modifie l'article 12 de la LPRPSP afin d'autoriser les entreprises à utiliser, sans le consentement des individus, les renseignements personnels qu'elles détiennent (i) à des fins compatibles avec celles pour lesquelles ils ont été recueillis (art. 12 al. 2(1)) et (ii) à des fins d'étude, de recherche ou de production de statistiques, à condition qu'ils soient dépersonnalisés (art. 12 al. 2(5)).

Fins compatibles. L'article 12 al. 2 (1) permettra aux entreprises d'utiliser les renseignements personnels pour une fin secondaire, sans devoir obtenir un consentement, à condition que cette finalité soit compatible avec les fins de la collecte. Une fin sera considérée « compatible » lorsqu'elle a un « lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli » et à condition que ce ne soit pas dans un but de « prospection commerciale ou philanthropique » (ex. marketing). Ces termes font écho au libellé utilisé dans d'autres lois canadiennes en matière de protection des renseignements personnels dans le secteur public et au RGPD qui prévoit qu'un traitement de données à caractère personnel pour d'autres fins que celles de la collecte ne devrait être autorisé « que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement ».

⚠ Même si cette nouvelle exception au consentement permet aux entreprises d'utiliser les renseignements personnels dans leur forme brute à des fins de recherche et d'analyse interne, elles doivent néanmoins faire preuve de prudence. En effet, la CAI peut se demander si l'utilisation à une fin secondaire correspond aux attentes raisonnables de l'individu plutôt que de se demander si cette utilisation est « objectivement » compatible avec les fins initiales. Plus les renseignements en cause sont sensibles, plus il est probable que la CAI adopte une posture fondée sur l'analyse des « attentes raisonnables ».

Par exemple, l'utilisation de renseignements personnels non sensibles dans le cadre d'analyses qui visent l'amélioration ou l'optimisation des services, non seulement pour l'individu, mais aussi pour tous les utilisateurs du service, pourrait être considérée comme une utilisation à des fins compatibles, à condition que l'entreprise ait mentionné cette utilisation dans sa politique de confidentialité. Or, l'utilisation de renseignements sensibles dans le même but d'amélioration générale des services peut excéder ce que la CAI considère comme étant ce à quoi les individus peuvent raisonnablement s'attendent. Il serait alors plus prudent d'utiliser des renseignements personnels dépersonnalisés comme données de base pour ces analyses (ce que prévoit également l'article 12 comme nous le verrons plus loin).

Étude ou recherche à partir de renseignements dépersonnalisés. L'article 12 al. 2(5) prévoit que l'utilisation d'un renseignement personnel sans consentement sera permise lorsque son utilisation est « nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé ». Étant donné que l'exception au consentement prévue à l'article 12 s'applique à l'utilisation des renseignements personnels au sein de l'entreprise, il est tout naturel d'interpréter les termes « étude » ou « recherche » comme englobant l'analyse commerciale. Toutefois, l'exception s'étend également à d'autres formes d'activités de recherche internes, notamment celles qui font appel à l'apprentissage automatique ou à d'autres techniques avancées d'analyse des données susceptibles d'être impliquées dans le développement de systèmes décisionnels automatisés (examinés plus en détail dans la section 4.3).

Notons que cette exception au consentement ne prévoit pas expressément que l'utilisation pourra s'effectuer à l'insu de l'individu. Cela dit, les exceptions au consentement énumérées à l'article 12 se situent sur un continuum où l'absence de connaissance va d'une situation sans réelle conséquence pour l'individu concerné (par exemple, utilisation manifestement au bénéfice de l'individu) à une situation réellement bénéfique pour les individus et l'entreprise (par exemple, utilisation dans un but de prévention et de détection de la fraude). En conséquence, on ne peut pas raisonnablement supposer que, de manière générale, les individus visés par les exceptions à l'exigence du consentement énumérées à l'article 12 seront informés de l'utilisation en question. Ceci est d'autant plus pertinent dans la mesure où l'utilisation de renseignements personnels dans des contextes d'apprentissage automatique non supervisé peut conduire à la découverte de nouveaux objectifs qui ne pouvaient raisonnablement pas être connus à l'avance.

Le nouvel article 12 prévoit qu'un renseignement personnel est « dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée » (art. 12 al. 4 (1)). Cette définition correspond essentiellement à la notion de « pseudonymisation » des données, telle qu'elle est généralement comprise (notamment dans le RGPD). À titre comparatif, la Loi 64 prévoit également des critères pour l'anonymisation des renseignements personnels en précisant que « [p]our l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier **directement** ou **indirectement** cette personne » (art. 23 [notre emphase]). Il est intéressant de noter que le libellé du nouvel article 12 prévoit aussi clairement qu'aucun consentement n'est nécessaire même lorsque ces renseignements sont sensibles préalablement à leur anonymisation (art. 12 al. 1 et 2).

Le nouvel article 12 reconnaît également le risque de réidentification lié aux renseignements dépersonnalisés en obligeant les entreprises qui les utilisent à prendre « les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés » (art. 12 al. 5). D'ailleurs, bien que cela ne soit pas expressément indiqué, il serait conforme à la définition des renseignements personnels sensibles prévue à l'article 12 al. 4 (2) (ainsi qu'aux orientations de la CAI et des autres commissaires canadiens à la protection de la vie privée) d'interpréter les « mesures raisonnables » comme nécessitant l'adoption de mesures supplémentaires ou plus rigoureuses lorsque les renseignements personnels sous-jacents aux renseignements dépersonnalisés sont sensibles.

Évaluations des facteurs relatifs à la vie privée. La recherche interne menée en vertu de l'art. 12 al. 2 (1) ou (5), peut nécessiter la réalisation d'une EFVP lorsqu'elle s'inscrit dans le cadre d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services (art. 3.3 al. 1) (voir la section 2.3).

Pistes de conformité

1. **Mettre en place une procédure pour s'assurer que, avant d'utiliser des renseignements personnels à des fins de recherche interne, l'entreprise a :**
   - obtenu le consentement pour cette utilisation;
   - déterminé que la finalité de la recherche est compatible avec la finalité pour laquelle les renseignements ont été recueillis; ou
   - dépersonnalisé (c'est-à-dire, au minimum, pseudonymisé) les renseignements personnels.
2. **Faire preuve de prudence lorsque l'entreprise se base sur l'exception des « fins compatibles » pour utiliser des renseignements personnels sensibles dans le cadre de recherches internes.** Lorsque les renseignements sont sensibles, la CAI peut se demander si l'utilisation à une fin secondaire correspond aux attentes raisonnables de l'individu plutôt que de se demander si cette utilisation est « objectivement » compatible avec les fins initiales.
3. **Prendre les mesures nécessaires pour réduire le risque de réidentification,** lorsque l'entreprise utilise des renseignements dépersonnalisés en vertu de l'exception pour les « fins d'étude ou de recherche ».
4. **Adopter des mesures plus rigoureuses pour éviter la réidentification** lorsque les renseignements personnels sous-jacents aux renseignements dépersonnalisés sont sensibles.
5. **Mettre en place une procédure visant à effectuer une évaluation des facteurs relatifs à la vie privée** si la recherche interne (en vertu de l'une ou l'autre des exceptions discutées) s'inscrit dans le cadre d'un « projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique ».

4.3. Prise de décision automatisée

En vigueur le 22 septembre 2023

Le nouvel article 12.1 introduit des obligations de notification pour les entreprises utilisant des renseignements personnels pour prendre une décision concernant un individu, qui est fondée **exclusivement** sur le traitement automatisé de ces renseignements. Il pourrait s'agir, par exemple, de situations où une entreprise décide d'accorder ou de refuser l'accès à un produit ou à un service en se basant sur l'évaluation de la situation financière ou médicale d'un client ou en utilisant un système biométrique.

Exigences en matière de notification et d'information. L'article 12.1 exige que les entreprises informent les individus du fait que leurs renseignements personnels sont utilisés pour prendre une décision fondée exclusivement sur un traitement automatisé, au plus tard au moment où l'individu est informé de la décision elle-même. D'un point de vue pratique, on peut penser que des avis distincts ou « juste à temps » pourraient être exigés en vertu des futures lignes directrices de la CAI. Les entreprises utilisant des technologies pour prendre des décisions basées exclusivement sur le traitement automatisé de renseignements personnels devraient indiquer cette utilisation dans leurs politiques de confidentialité.

L'article 12.1 oblige également les entreprises à informer, sur demande, l'individu visé par une telle décision :

- des renseignements personnels utilisés pour rendre la décision;
- des raisons ainsi que des principaux facteurs et paramètres ayant mené à la décision;
- du droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

Notons que la formulation utilisée ne limite pas ces droits aux renseignements personnels qui concernent l'individu. Il n'est pas certain que cela soit intentionnel, compte tenu du contexte : les technologies d'apprentissage automatique (« machine learning ») qui prennent des décisions concernant des individus peuvent avoir besoin d'ingérer une multitude de renseignements personnels provenant de nombreux individus afin de produire un modèle capable de prendre des décisions précises. Bien qu'aucune interprétation de la loi n'exige que les renseignements personnels d'autres individus soient divulgués à l'individu visé par la décision d'un tel système, il se pourrait que les entreprises soient tenues de divulguer la nature de tous les renseignements personnels utilisés (par exemple, le fait qu'à la phase de mise au point on ait utilisé les noms de criminels reconnus coupables et les codes postaux de leur lieu de résidence). La formulation « informer [la personne concernée] des renseignements personnels utilisés » est ambiguë à cet égard. Les directives de la CAI seront d'une importance capitale pour comprendre comment cette obligation devra être appliquée.

L'expression « traitement automatisé » n'est pas définie dans la Loi 64. D'éventuelles lignes directrices de la CAI seront donc essentielles pour circonscrire la portée des exigences introduites à l'article 12.1. Bien que les modifications introduites par la Loi 64 semblent viser la prise de décision automatisée au moyen d'algorithmes technologies d'intelligence artificielle (IA) et dont l'incidence sur

les droits individuels est majeure, le libellé de cette disposition est rédigé de façon suffisamment large pour inclure toutes sortes d'autres processus automatisés de prise de « décision ».
Par exemple, l'article 12.1 n'exclut pas la décision, prise à l'issue d'un processus automatisé, de présenter une offre, un produit ou un service à un individu en fonction de son activité en ligne ou de ses intérêts (par ex. la publicité ciblée).

La CAI a fait du traitement automatisé l'un des thèmes de son « Espace évolutif » sur le projet de loi n° 64, ce qui illustre son intention d'émettre certaines lignes directrices à ce sujet. Il est donc raisonnable pour les entreprises de s'attendre à la publication de telles orientations d'ici l'entrée en vigueur de l'article 12.1. Il convient de mentionner que le terme « traitement automatisé » semble être repris du RGPD et pourrait donc être interprété de manière similaire. En Europe, le Groupe de travail « Article 29 » sur la protection des données a émis, avant l'entrée en vigueur du règlement, des lignes directrices sur l'interprétation des dispositions du RGPD régissant le traitement automatisé (voir Groupe de travail « Article 29 » sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement 2016/679). Notons que l'interprétation formulée par le Groupe de travail a été facilitée par le libellé restrictif des dispositions du RGPD qui visent un traitement automatisé « produisant des effets juridiques à l'égard d'une personne physique » ou « l'affectant de manière significative ». Le nouvel article 12.1 ne comporte pas de telles restrictions, ce qui compliquera sans doute le travail d'interprétation de la CAI. En l'absence de lignes directrices, les entreprises peuvent toutefois se préparer aux nouvelles obligations de notification et d'information prévues par la loi en envisageant de suivre avec prudence l'interprétation retenue dans le contexte européen pour déterminer si et dans quelles circonstances une technologie sera considérée comme un « traitement automatisé ».

L'obligation d'informer l'individu « des raisons » ayant mené à la décision semble équivaloir d'exiger une explication de la décision automatisée. Comme cela a été abondamment discuté dans la littérature au sujet de l'IA, les processus utilisés par les modèles d'apprentissage automatique pour parvenir à leurs résultats sont reconnus pour leur opacité. Dans de nombreux cas, l'explication fournie est soit superficielle au point d'être vide de sens ou bien si technique qu'elle est incompréhensible pour l'individu moyen. Bien que la mention des « principaux facteurs et paramètres » donne une indication quant au niveau de détail requis, les entreprises doivent, en l'absence de lignes directrices, faire preuve de prudence afin d'éviter de communiquer des renseignements qui pourraient (i) divulguer des secrets commerciaux ou violer le droit de propriété intellectuelle de l'entreprise ou de tiers (comme les fournisseurs de services qui fournissent la technologie de traitement automatisé) ou (ii) permettre à des tiers mal intentionnés de s'infiltrer dans leur système.

Droit de présenter des observations. En outre, l'individu qui fait l'objet de la décision automatisée doit avoir « l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision ». Les activités de traitement automatisé qui visent des individus doivent donc, sur demande, être examinées par du personnel ayant le pouvoir (et, vraisemblablement, les connaissances suffisantes) de réévaluer les décisions prises par le système. Il est intéressant de noter que l'article 12.1 n'accorde pas aux individus un droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (comme celui prévu à l'article 22 du RGPD), mais uniquement un droit de « présenter ses observations ». Ceci semble accorder au personnel chargé de la révision une grande latitude dans son évaluation de la décision automatisée après réception des observations de l'individu. En d'autres termes, l'entreprise ne semble pas avoir d'obligation distincte de délibérer et de parvenir

à une conclusion indépendante ou de fournir une justification quant à son choix de réviser ou non la décision. Les entreprises seront donc en mesure de trier les demandes non fondées et ainsi éviter les frais administratifs importants liés à la gestion de telles demandes. Néanmoins, elles doivent être prêtes à évaluer les observations soumises par les individus et à agir de manière appropriée lorsque l'examen de la décision et des observations révèle clairement un problème dans le processus de traitement automatisé ou la manière dont les renseignements personnels sont utilisés.

Pistes de conformité

1. **Se préparer à agir en fonction des orientations qui seront publiées par la CAI concernant l'interprétation de la notion de « traitement automatisé ».** En l'absence de telles orientations, les entreprises peuvent avec prudence envisager de suivre l'interprétation donnée au « traitement automatisé » en vertu du RGPD.
2. **Mettre en place une procédure pour s'assurer que lorsqu'une entreprise prend des décisions fondées exclusivement sur le traitement automatisé de renseignements personnels, elle verra à :**
   - En informer les individus par l'entremise de sa politique de confidentialité;
   - Mettre en place une procédure conformément aux Pistes de conformité prévues dans la section 5.
3. **Faire preuve de prudence dans la communication des raisons ayant mené à la décision, qui pourraient :**
   - Révéler des secrets commerciaux ou violer les droits de propriété intellectuelle de l'entreprise ou de tiers (comme les fournisseurs de technologies de traitement automatisé);
   - Permettre à des tiers mal intentionnés d'infiltrer le système.
4. **Se préparer à évaluer les observations des individus relatives à une décision prise par traitement automatisé** et à agir de manière appropriée lorsque l'examen de la décision et des observations révèle clairement un problème dans le processus de traitement automatisé ou la manière dont les renseignements personnels sont utilisés.

5. Nouveaux droits individuels

Les individus se voient accorder trois nouveaux droits en vertu de la Loi 64 : un droit de contrôler la diffusion de leurs renseignements personnels (également connu sous le nom de « droit à l'oubli »), un droit à la portabilité des données et un droit d'être informé d'une prise de décision automatisée et de soumettre des observations. En outre, la Loi 64 renforce le contrôle individuel et les droits existants en matière de protection des renseignements personnels en permettant aux individus de demander aux entreprises des informations supplémentaires sur le traitement de leurs données.

5.1. Droit à l'oubli

En vigueur le 22 septembre 2023

La Loi 64 donne aux individus le droit de contrôler la diffusion de leurs renseignements personnels, notamment par les entreprises qui facilitent la diffusion de ces renseignements. Ce droit, également connu sous le nom de droit à l'oubli, a pour principal objectif de renforcer le contrôle des individus sur leur réputation et leur vie privée en ligne en limitant l'accès du public aux renseignements personnels lorsque leur diffusion est illégale (par exemple, la pornographie vengeresse ou *revenge porn*) ou porte gravement atteinte à la réputation ou à la vie privée. Contrairement au droit équivalent prévu par le RGPD, le nouveau droit à l'oubli du Québec n'est pas un droit à l'effacement des renseignements personnels en soi, mais plutôt un droit plus limité de restreindre la diffusion des renseignements. Notons au passage que le droit de demander la suppression des renseignements personnels est maintenu par la Loi 64, conformément à l'article 28 de la LPRPSP et à l'article 40 du CCQ. Pour plus de détails sur le droit à la suppression, veuillez vous référer à notre bulletin *Le droit à la suppression des renseignements personnels au Canada : entre réalité et fiction*.

Portée du droit à l'oubli. En vertu de ce nouveau droit, un individu peut empêcher une entreprise de diffuser ses renseignements personnels ou peut demander à ce que soit désindexé (ou, pour être plus précis, « déréférencer » des résultats de recherche) un hyperlien rattaché à son nom permettant d'accéder à un renseignement personnel, lorsque la diffusion de ce renseignement (i) contrevient à la Loi ou à une ordonnance judiciaire ou (ii) cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée (art. 28.1). En pratique, cela signifie qu'une entreprise qui reçoit ce type de demande doit non seulement conclure que le préjudice existe réellement et qu'il n'est pas simplement hypothétique ou potentiel, mais aussi qu'il l'emporte sur le droit du public à l'information et sur la liberté d'expression de l'éditeur ou du créateur de contenu, et que la mesure demandée n'est pas excessive pour empêcher la perpétuation du préjudice. Pour faire cette évaluation, l'entreprise doit spécifiquement prendre en compte un certain nombre de facteurs prescrits, qui reflètent étroitement ceux élaborés dans les décisions relatives à la diffamation ou aux demandes liées à la vie privée. Ces facteurs sont les suivants :

- Le statut de personnalité publique de l'individu;
- Le fait que le renseignement concerne un individu alors qu'il était mineur;

- L'exactitude, le caractère actuel et la sensibilité des renseignements personnels diffusés;
- Le contexte de sa diffusion;
- Le temps écoulé depuis sa diffusion; et
- Si les renseignements concernent une procédure criminelle ou pénale, l'obtention d'un pardon ou l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires.

⚠ Il est intéressant de noter que ce nouveau droit prévoit la possibilité de « réindexer » les hyperliens rattachés au nom d'un individu lorsque cela peut empêcher une atteinte grave à la réputation ou à la vie privée d'une personne. Selon les commentaires de la ministre Sonia LeBel, le droit de réindexer les hyperliens peut être compris comme un droit de « déplacer » un hyperlien, ce qui peut soulever un certain nombre de problèmes pratiques.

Format de la demande. Une entreprise ne doit prendre en considération que les demandes formulées par écrit par un individu qui prouve qu'il est bel et bien la personne concernée par les renseignements personnels ou par un représentant autorisé, tel qu'un titulaire de l'autorité parentale (art. 30).

⚠ Bien que la LPRPSP donne aux héritiers, aux successeurs, aux liquidateurs d'une succession et à un certain nombre d'autres personnes la possibilité d'exercer le droit d'accès ou de rectification d'une personne décédée, il n'est pas clair si cette autorisation vaut également pour le droit à l'oubli.

Évaluation du bien-fondé de la demande. Étant donné que le demandeur est généralement mieux placé pour apporter des éléments de preuves à l'appui de sa demande, c'est à ce dernier qu'incombe le fardeau d'établir que la diffusion des renseignements personnels est en fait illégale ou qu'elle cause un préjudice grave à sa réputation ou à sa vie privée. Toutefois, des lignes directrices pourraient être nécessaires pour confirmer ce point. L'entreprise qui reçoit une telle demande doit alors faire preuve de diligence raisonnable pour évaluer la validité de la demande et requérir des éclaircissements au demandeur si nécessaire. Il reste à voir si cette exigence requiert réalisation d'une enquête indépendante ou un exercice de collecte de faits. Elle soulèvera probablement des questions plus larges sur le rôle des entreprises privées dans la détermination des renseignements auxquels le public a un intérêt légitime à y accéder. Comme ce rôle a traditionnellement été rempli par les tribunaux, qui sont généralement mieux placés pour résoudre des questions complexes de fait et de droit et sont soumis à diverses garanties procédurales destinées à protéger les droits fondamentaux concurrents, des contestations relatives à la constitutionnalité du droit à l'oubli introduit par la Loi 64 pourraient éventuellement survenir.

Délai de réponse à la demande. Le responsable de la PRP doit répondre à la demande par écrit dans les 30 jours suivants sa réception (art. 32). Cependant, l'entreprise peut soumettre une demande à la CAI dans cette période initiale de 30 jours pour prolonger le délai de réponse (art. 46). Contrairement à d'autres lois canadiennes en matière de protection des renseignements personnels, aucune limite n'est fixée concernant le nombre total de jours pour lequel la CAI peut prolonger le délai.

Accueillir la demande. Lorsque la demande est accueillie, le responsable de la PRP doit répondre par écrit et fournir une attestation que les renseignements ne sont plus diffusés ou que l'hyperlien a été désindexé ou réindexé, selon le cas (art. 28.1 al. 5).

Refuser la demande. Lorsque la demande est refusée, le responsable de la PRP doit répondre par écrit, motiver le refus, indiquer la disposition sur laquelle le refus est fondé (le cas échéant) et informer le demandeur des recours qui lui sont disponibles et du délai pour les exercer (s. 34). Sur ce dernier point, l'entreprise doit informer le demandeur de son droit de soumettre une demande d'examen de mésentente à la CAI dans les 30 jours suivant le refus d'accéder à la demande (art. 43). Sur demande, le responsable de la PRP doit également aider le demandeur à comprendre le refus.

Questions en suspens. Si le droit à l'oubli prévu par la Loi 64 semble viser les moteurs de recherche et les éditeurs de contenu, la situation est moins claire en ce qui concerne les intermédiaires en ligne qui ne font que faciliter la diffusion de contenus générés par les utilisateurs sans jouer un rôle actif dans leur publication (comme les réseaux sociaux). La question de savoir si l'on peut dire qu'ils « diffusent » l'information qui circule sur leurs plateformes soulève d'importantes questions quant à leur rôle et à leurs responsabilités en matière de surveillance du contenu généré par les utilisateurs, en particulier à la lumière des protections offertes par les articles 22 et 27 de la *Loi concernant le cadre juridique des technologies de l'information* (« **LCCJTI** »). Sur ce dernier point, la Cour supérieure du Québec, dans l'affaire *Lehouillier-Dumas c. Facebook inc.*, 2021 QCCS 2074, apporte des précisions intéressantes sur ces questions plus larges.

5.2. Droit à la portabilité des données

En vigueur le 22 septembre 2024

Considérée comme une extension au droit d'accès, la portabilité des données accorde aux individus un droit supplémentaire de recevoir les renseignements personnels informatisés recueillis auprès d'eux dans un **format technologique structuré et couramment utilisé**, et de voir ces renseignements transférés directement à « toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement » (art. 27 al. 3). Ces renseignements doivent également être communiqués sous la forme d'une transcription écrite et intelligible (art. 27 al. 2). Ainsi, l'objectif du droit à la portabilité des données semble être de faciliter la réutilisation des données et d'améliorer la capacité des consommateurs à changer de fournisseur, ce qui renforce leur contrôle individuel sur leurs renseignements personnels et favorise une plus grande concurrence. Bien que le droit à la portabilité des données ne vise pas nécessairement l'interopérabilité entre les systèmes, celle-ci est souvent présentée comme l'un de ses objectifs sous-jacents.

Signification d'un « format technologique structuré et couramment utilisé ». Les termes « structuré », « couramment utilisé » et « technologique » ne sont pas explicitement définis dans la Loi, et leur signification est susceptible de varier selon l'industrie ou le secteur concerné. Dans l'UE, l'ancien Groupe de travail Article 29 a publié des directives dans lesquelles il a estimé que les formats ouverts tels que CSV, XML et JSON, accompagnés de métadonnées utiles à la compréhension de leur signification, étaient conformes au droit de portabilité des données du RGDP lorsqu'aucun format communément utilisé n'était disponible. Cela dit, des lignes directrices seront nécessaires pour confirmer quels formats peuvent être considérés conformes aux exigences de la Loi 64.

Portée du droit à la portabilité des données. Le droit à la portabilité des données ne s'applique qu'aux renseignements personnels informatisés qui ont été recueillis auprès de l'individu. En d'autres termes, il ne s'applique pas aux renseignements détenus dans un format non informatisé, comme des documents papier, ou recueillies auprès d'un tiers. Afin de protéger les intérêts commerciaux des entreprises, y compris les algorithmes utilisés pour générer des données inférées, le droit à la portabilité des données exclut expressément de son champ d'application les renseignements personnels qui ont été créés ou inférés à partir des renseignements recueillis auprès de l'individu. Les données inférées peuvent par exemple prendre la forme de déductions sur la probabilité qu'un client achète certains produits ou services ou encore la probabilité qu'il soit intéressé à recevoir du contenu publicitaire particulier. Il convient de noter que la mise en œuvre de ce droit doit également être prise en compte lors de l'acquisition, du développement ou de la refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication ou la destruction de renseignements personnels (art. 3.3 al. 3) (voir la section 2.3). Bien qu'une plus grande clarté soit nécessaire en ce qui concerne certains aspects procéduraux associés au droit à la portabilité des données, son inclusion dans l'article traitant du droit d'accès suggère que les entreprises devraient traiter les demandes de portabilité des données conformément au régime actuel applicable aux demandes d'accès aux renseignements personnels.

Exemptions à la portabilité des données. Lorsque la fourniture des renseignements dans un format technologique structuré et couramment utilisé « soulève des difficultés pratiques sérieuses » pour l'entreprise qui reçoit la demande, cette dernière peut être exemptée de l'obligation de se conformer à cette exigence (art. 27 al. 3). En outre, le droit à la portabilité des données ne saurait s'appliquer aux renseignements qui sont autrement exemptés du droit d'accès, car la portabilité des données est considérée comme une extension de ce dernier (voir les articles 37 à 41). En ce sens, les renseignements personnels informatisés dont la divulgation serait susceptible de révéler des renseignements personnels sur une tierce personne sont susceptibles d'être exclus des exigences d'accès et de portabilité en vertu de l'article 40 de la LPRPSP.

Enfin, il est important de noter que le droit à la portabilité des données est la seule disposition de la Loi 64 à entrer en vigueur le 22 septembre 2024, soit trois ans après la sanction de la loi.

5.3. Droit d'être informé d'une décision automatisée et de soumettre des observations

En vigueur le 22 septembre 2023

La Loi 64 accorde aux individus trois nouveaux droits en ce qui concerne la prise de décision automatisée impliquant des renseignements personnels, à savoir (i) le droit d'en être informé, (ii) le droit de demander des informations supplémentaires sur la prise de décision automatisée, et (iii) le droit de soumettre des observations à une personne désignée au sein de l'entreprise. Il convient de souligner que ces droits sont limités aux décisions basées « exclusivement » sur un traitement automatisé des renseignements personnels d'un individu, excluant ainsi les décisions basées sur une combinaison de traitement automatisé et d'intervention humaine significative.

Droit d'être informé de la prise de décision automatisée. Les individus ont le droit d'être informés du fait que leurs renseignements personnels sont utilisés pour prendre une décision fondée exclusivement sur un traitement automatisé. Voir la section 4.3 pour plus de détails sur cette nouvelle exigence.

Droit de demander de l'information supplémentaire sur la décision automatisée. Les individus peuvent également demander des renseignements additionnels concernant la décision automatisée. Ils sont notamment en droit de connaitre les renseignements personnels qui ont été utilisés pour rendre la décision, les raisons et les principaux facteurs et paramètres ayant mené à la décision et leur droit de faire rectifier les renseignements personnels utilisés pour rendre la décision. Voir la section 4.3 pour plus de détails sur cette nouvelle exigence. Étant donné qu'aucune modalité n'est imposée à l'exercice du droit de demander de l'information supplémentaire, un individu peut être autorisé à soumettre une demande verbalement ou par écrit. L'entreprise doit néanmoins agir avec diligence et conserver un dossier de ce type de demande, y compris la réponse de l'entreprise à celle-ci, car le non-respect de cette exigence – ou de tout autre droit accordé en vertu de l'article 12.1 – peut donner lieu à l'imposition de sanctions administratives pécuniaires (art. 90.1(4)) (voir section 1).

Droit de présenter des observations à une personne désignée au sein de l'entreprise. Les individus doivent avoir la possibilité de présenter leurs observations à un membre du personnel de l'entreprise, et cette personne désignée doit être en mesure de réviser la décision. Voir la section 4.3 pour plus de détails sur cette nouvelle exigence.

5.4. Droit d'obtenir des renseignements sur le traitement des données

En vigueur le 22 septembre 2023

La Loi 64 permet aux individus de demander de l'information sur le traitement de leurs données, à savoir quels renseignements personnels ont été recueillis auprès d'eux et comment ils sont traités par l'entreprise. En particulier, un individu pourrait demander à recevoir non seulement les informations qui lui ont été fournies au moment de la collecte, mais aussi des informations supplémentaires, comme les catégories de personnes qui ont accès à ses renseignements personnels au sein de l'entreprise, la période de conservation applicable et les coordonnées du responsable de la PRP (art. 8). Si les renseignements personnels d'un individu ont été recueillis auprès d'un tiers, l'individu peut également demander à être informé de la source des renseignements, sauf si les renseignements ont été recueillis dans le cadre d'une enquête visant à prévenir, à détecter ou à réprimer un crime ou une infraction à la loi (art. 7). Pour plus de détails sur ces exigences, veuillez vous référer à la section 3.1. D'autres lois canadiennes en matière de protection des renseignements personnels accordent aux individus un droit similaire d'obtenir des renseignements sur le traitement des données. Toutefois, ce droit s'inscrit dans le cadre du droit d'accès, ce qui signifie qu'une entreprise qui reçoit ce type de demande doit la traiter conformément à la procédure et aux délais applicables à une demande d'accès. En revanche, la Loi 64 sépare ces deux droits, créant ainsi un régime plus souple pour les demandes faites en vertu des articles 7 et 8. Il est néanmoins recommandé d'agir avec diligence, car le fait de ne pas informer les individus conformément à ces dispositions est l'une des situations énumérées qui donnent lieu expressément à l'imposition de sanctions administratives pécuniaires (art. 90.1(1)) (voir la section 1).

Pistes de conformité

1. **Dresser un inventaire des pratiques susceptibles de faire intervenir les nouveaux droits individuels** afin de déterminer si ces pratiques relèvent de l'une des situations suivantes:
   - L'entreprise diffuse un contenu susceptible de contenir des renseignements personnels ou exploite un outil de recherche en ligne ou un service d'indexation similaire qui génère des résultats de recherche (sous forme d'hyperliens) sur la base du nom d'une personne.
   - L'entreprise rend des décisions fondées exclusivement sur un traitement automatisé des renseignements personnels.
   - L'entreprise collecte des renseignements personnels informatisés auprès d'individus.
2. **Dresser un inventaire des politiques et procédures existantes pour le traitement des demandes relatives à la vie privée** ou de tout document similaire (clients ou employés) **et les examiner** pour s'assurer que:
   - L'entreprise est capable de reconnaître et de répondre à une demande (verbale ou écrite) d'information sur le traitement des données.
   - L'entreprise est en mesure de fournir, sur demande, des renseignements personnels informatisés à l'individu, ou à une personne ou une entreprise autorisée par la loi à recueillir de tels renseignements, dans un format technologique structuré et couramment utilisé.
3. **Si elle rend des décisions fondées exclusivement sur un traitement automatisé, mettre en place une procédure pour s'assurer que:**
   - L'entreprise est en mesure d'informer les individus (clients ou employés) de ce fait au plus tard au moment où elle les informe de la décision.
   - L'entreprise est capable de reconnaître et de répondre à une demande (verbale ou écrite) d'information sur la prise de décision automatisée.
   - L'entreprise a désigné un membre de son personnel qui est en mesure de réviser ces décisions et qui est chargé de recevoir les observations des individus.

→ Suite à la page suivante

Pistes de conformité

4. **Si elle diffuse des renseignements personnels ou exploite un outil de recherche en ligne, mettre en place une procédure pour garantir que:**

    - L'entreprise est en mesure de recevoir, d'évaluer et de répondre à une demande de droit à l'oubli dans les délais prescrits.
    - L'entreprise a mis en place un processus lui permettant de déterminer si la diffusion des renseignements personnels (i) contrevient à la loi ou à une ordonnance judiciaire ou cause un préjudice grave au droit de l'individu au respect de sa réputation ou de sa vie privée; et (ii) le cas échéant, cause un préjudice qui l'emporte sur le droit du public à l'information et sur la liberté d'expression de l'éditeur ou du créateur de contenu.
    - L'entreprise est en mesure de vérifier l'identité du demandeur qui fait la demande (conformément aux lois applicables).
    - L'entreprise est en mesure de fournir des attestations (si la demande est acceptée) que les renseignements ne sont plus diffusés ou que l'hyperlien a été désindexé ou réindexé, selon le cas.

6. Impartition et transfert de renseignements personnels à l'extérieur du Québec

La Loi 64 introduit de nouvelles exigences en matière d'impartition et de communication de renseignements à l'extérieur du Québec.

6.1. Impartition

En vigueur le 22 septembre 2023

Transparence. Tel qu'indiqué à la section 3.1, la Loi 64 requiert que l'entreprise indique à l'individu, au moment de la collecte et par la suite sur demande, le nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins décrites dans la politique de confidentialité de l'entreprise (art. 8 al. 2). Ceci implique que, désormais, la politique de confidentialité de l'entreprise devra indiquer que les renseignements personnels pourront être transmis à ses fournisseurs de service (catégorie de tiers) ou nommer ceux-ci individuellement.

Exception au consentement. Tel qu'indiqué à la section 3.3, la Loi 64 permet la communication de renseignements personnels à un tiers sans le consentement de l'individu concerné, lorsque cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise (art. 18.3). Cette exception permet donc à l'entreprise de transmettre des renseignements personnels à ses mandataires et fournisseurs de services (« fournisseur de services ») sans que l'individu n'ait à consentir à ceci.

Obligation d'effectuer une EFVP. Lorsqu'un projet d'impartition comprend l'acquisition, le développement ou la refonte d'un système d'information ou d'une prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels par un fournisseur de services pour le compte de l'entreprise, celle-ci devra procéder à une EFVP (art. 3.3 al. 1). Bien que cette responsabilité incombe à l'entreprise, le fournisseur de services devrait collaborer à cet exercice. Nous référons à la section 2.3 pour les exigences relatives aux EFVP.

Entente écrite. La Loi 64 requiert en outre que le traitement de renseignements personnels par un fournisseur de services soit sujet à un contrat écrit devant comprendre les mesures que le fournisseur de services doit prendre pour assurer:

- la protection du caractère confidentiel du renseignement personnel communiqué. Le contrat devrait donc prévoir les mesures physiques, organisationnelles et techniques devant être mises en place par le fournisseur de service traitant les renseignements, que ceux-ci soient en transit ou stockés;
- que ce renseignement ne soit utilisé que dans le cadre de l'exécution du contrat. Le contrat devrait donc prohiber l'utilisation des renseignements personnels par le fournisseur pour ses fins propres ou pour les fins d'un tiers. Il serait utile de clarifier si les nouvelles exceptions au consentement prévues à l'article 12 permettraient néanmoins au fournisseur de services d'utiliser les renseignements pour les fins qui y sont décrites (par exemple, dépersonnaliser les renseignements pour les utiliser à des fins internes de recherche ou de production de statistiques).

- que le fournisseur de service ne conserve pas les renseignements personnels après l'expiration du contrat. La Loi 64 ne précise pas si l'anonymisation de ces renseignements par les fournisseurs de services afin de les utiliser pour poursuivre leurs fins sérieuses et légitimes (art. 23) permettrait de satisfaire cette exigence.

Obligation de notifier les violations des obligations de confidentialité. L'article 18.3 requiert également que le fournisseur de service avise sans délai le responsable PRP de l'entreprise de « toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué », et non simplement les incidents de confidentialité. Il n'est pas clair si les parties pourront aménager les conditions auxquelles cette obligation sera soumise le cas échéant, par exemple pour limiter l'obligation de notification aux seuls « incidents de confidentialité ».

Autoriser les vérifications par l'entreprise. Le fournisseur de services doit permettre au responsable de la PRP d'effectuer toute vérification relative aux obligations de confidentialité du fournisseur, c'est-à-dire de demander tout document et effectuer toute vérification additionnelle. Il n'est pas clair si les parties pourront aménager les conditions auxquelles ces obligations seront soumises le cas échéant, par exemple en exigeant que les vérifications soient faites à certains moments ou soumises à certaines conditions.

Ces deux obligations (entente écrite et obligation de notifier les violations des obligations de confidentialité) ne s'appliquent pas lorsque le fournisseur de services est un organisme public au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ou un membre d'un ordre professionnel (art. 18.3 al. 3).

Pistes de conformité

1. **Politique de confidentialité.** Réviser la politique de confidentialité de l'entreprise pour s'assurer qu'elle indique que les renseignements personnels pourront être transmis à ses fournisseurs de service. Si l'entreprise le souhaite, la politique pourra nommer ces fournisseurs.
2. **Développer une procédure d'impartition** qui régit les employés susceptibles de sous-traiter le traitement de renseignements personnels (par exemple, l'équipe chargée de l'approvisionnement).
3. **Préparer un modèle de contrat (ou de clauses) de traitement des renseignements personnels.** Ce contrat devra prévoir :
   - la protection des renseignements personnels;
   - l'utilisation des renseignements personnels aux fins de l'exécution du contrat;
   - la destruction des renseignements à l'issue du contrat;

→ Suite à la page suivante

Pistes de conformité

- l'obligation pour le fournisseur de services de notifier sans délai l'entreprise en cas de violation ou tentative de violation des obligations de confidentialité; et
- la possibilité pour l'entreprise de demander tout document et d'effectuer toute vérification relative à la confidentialité des renseignements.

4. **Recenser les fournisseurs de services traitant des renseignements personnels pour l'entreprise.** L'entreprise devra alors :
   - Déterminer si un contrat écrit conforme aux exigences de la piste 2 a bien été conclu avec chaque fournisseur de service; et
   - Dans la négative, transmettre le modèle de contrat de traitement des renseignements personnels décrit à la piste 3 ci-dessus aux fournisseurs de services concernés.
5. **Communiquer avec les fournisseurs de service existants dont les systèmes/ prestations requièrent que l'entreprise mène une EFVP.** Sur la base de la liste mentionnée à la piste 4 ci-dessus, l'entreprise devrait prévoir de:
   - Communiquer avec chaque fournisseur de services existant que l'entreprise souhaite impliquer dans l'acquisition, le développement ou la refonte de systèmes ou prestations de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels pour leur indiquer que l'entreprise va mener une EFVP pour laquelle elle aura besoin de sa collaboration; et
   - Lorsque le modèle d'EFVP aura été développé par l'entreprise, celui-ci devrait être transmis aux fournisseurs de service pour qu'ils aident l'entreprise à compléter les informations factuelles et techniques relatives aux systèmes / services concernés.
6. **Effectuer les EFVP.** Une EFVP devra être menée par l'entreprise pour chaque projet d'impartition impliquant l'acquisition, le développement ou la refonte d'un système d'information ou d'une prestation électronique de services impliquant le traitement de renseignements personnels.

6.2. Transferts hors Québec

En vigueur le 22 septembre 2023

Transparence. Tel qu'indiqué à la section 3.1, l'entreprise qui collecte des renseignements personnels auprès d'individus doit les informer de la possibilité que ces renseignements soient communiqués à l'extérieur du Québec (et non simplement du Canada). Cette information devra être fournie au moment de la collecte et sur demande (art. 8 al.2).

Évaluation des facteurs relatifs à la vie privée. Les transferts de renseignements personnels à l'extérieur du Québec sont une préoccupation majeure de la Loi 64, qui introduit, à l'article 17, des restrictions à ceux-ci. Ainsi, une entreprise qui (1) souhaite communiquer des renseignements personnels à l'extérieur du Québec ou (2) confie à un tiers situé à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des renseignements personnels est tenue d'effectuer une EFVP qui tient compte des facteurs suivants :

- la sensibilité des renseignements,
- la finalité de leur utilisation,
- les mesures de protection, y compris contractuelles, qui s'y appliqueront, et
- le régime juridique applicable dans l'État de réception, notamment les principes de protection des renseignements personnels qui y sont applicables. Il est à noter que la Loi 64 fait référence à des « principes », et non à une « loi » sur la protection des données.

Si l'EFVP « démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus » alors le transfert sera autorisé. Notons que la Loi ne précise pas en quoi consistent les « principes de protection des renseignements personnels généralement reconnus ». On peut se demander si cette notion est identique aux principes de protection personnels énumérés par la CAI dans son *Guide d'accompagnement pour réaliser une EFVP*, soit:

- Déterminer les fins de la collecte
- Limiter la collecte de renseignements personnels
- Informer la personne concernée
- Mettre en place des mesures de sécurité appropriées
- Limiter l'accès aux renseignements personnels
- Limiter l'utilisation de renseignements personnels
- Obtenir le consentement à communiquer des renseignements personnels
- Requérir le consentement des personnes concernées
- Assurer la qualité des renseignements personnels
- Permettre l'exercice des droits d'accès et de rectification
- Répondre avec diligence

Cette nouvelle approche ressemble aux exigences du RGPD qui exigent qu'une entreprise transférant des données à caractère personnel hors de l'Espace Économique Européen vers une juridiction n'ayant pas été reconnue adéquate par la Commission Européenne, effectue une évaluation des risques de transfert avant de transférer ces données à l'étranger (voir sur ce point les Recommandations 01/2020 et 02/2020 du *European Data Protection Board*) et ajoute le cas échéant toute mesure supplémentaire de protection aux clauses contractuelles types adoptées par la Commission européenne.

Entente écrite. Si l'EFVP démontre que les renseignements traités à l'étranger feront l'objet d'une protection adéquate, l'entreprise doit conclure avec le tiers une entente écrite qui tient compte, notamment :

- des résultats de l'EFVP et,
- le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation (art. 17 al. 2).

Ainsi, si l'EFVP conclut que les renseignements traités à l'étranger par un fournisseur de services seront suffisamment protégés avec un contrat reprenant les exigences de l'article 18.3, aucune autre mesure ne sera nécessaire. Si en revanche l'évaluation conclut que le traitement à l'étranger crée un risque pour leur protection, alors les parties devront convenir de mesures permettant de réduire ce risque à un niveau adéquat. La Loi ne précise pas en quoi consisterait ce type de mesures, mais on peut imaginer que des mesures techniques (ex : cryptage, dépersonnalisation), organisationnelles et contractuelles (ex : restrictions au partage des renseignements avec des autorités gouvernementales étrangères) pourraient être de nature à atténuer le niveau de risque. La Loi ne précise pas non plus ce qu'il adviendrait si le résultat de l'EFVP était défavorable, laissant penser que le transfert ne pourrait avoir lieu.

Pistes de conformité

1. **Réviser la politique de confidentialité de l'entreprise pour préciser que les renseignements personnels pourront être communiqués à l'extérieur du Québec** (et non simplement du Canada).

2. **Effectuer une cartographie des renseignements communiqués en dehors du Québec.** Cet exercice permettra d'obtenir une description des flux de renseignements. L'entreprise devra notamment vérifier :
   - L'adresse de l'entité impliquée dans la communication;
   - Les modalités selon lesquelles les affiliés et/ou sous-traitants de l'entité qui sont situés dans d'autres juridictions pourront avoir accès aux renseignements (par exemple, dans le cadre d'un service sous-traité vers une filiale située dans un pays tiers); et
   - La nature et le volume de renseignements personnels traités en dehors du Québec.

3. **Compléter le modèle d'EFVP pour évaluer les risques associés à la communication de renseignements personnels hors du Québec.** Ce modèle devra prendre en compte:
   - La sensibilité des renseignements communiqués;
   - La finalité de leur utilisation;
   - Les mesures de protection, y compris contractuelles, qui s'y appliqueront; et
   - Le régime juridique applicable dans l'État de réception.

→ Suite à la page suivante

Pistes de conformité

4. **Mener une EFVP pour les activités de traitement impliquant la communication de renseignements personnels en dehors du Québec.** Cet exercice devra notamment évaluer si le cadre juridique de chacune des juridictions dans lesquelles les renseignements seront traités dispose de principes de protection des renseignements personnels conformes aux « principes de protection des renseignements personnels généralement reconnus ».
    - Dans un premier temps, faute d'indication plus précise sur ce point, les entreprises pourront vérifier si la législation de État en question respecte les principes de protection de la vie privée figurant dans le *Guide d'accompagnement pour réaliser une EFVP*.
5. **Adapter son modèle de contrat (ou de clauses) relatif au traitement des renseignements personnels pour prendre en compte les exigences liées aux fournisseurs de services situés hors du Québec.** Ce modèle devra :
    - Refléter les exigences de l'article 18.3 décrites à la section 6.1, et
    - Prévoir des mesures de protection modulables en fonction des résultats de l'EFVP.
6. **Préparer un modèle de contrat (ou de clauses) avec les tiers non fournisseurs de services situés hors du Québec.** Ce modèle devra :
    - Imposer aux tiers de respecter les principes de protection des renseignements personnels généralement reconnus; et
    - Prévoir des mesures de protection modulables en fonction des résultats de l'EFVP.
7. **Compléter la procédure d'impartition décrite à la section 6.1** pour refléter les exigences liées à la communication de données en dehors du Québec.

7. Cybersécurité, gestion des incidents de confidentialité et biométrie

Le nouveau régime renforce l'obligation des entreprises d'assurer la protection des renseignements personnels à l'aide de nouvelles mesures de protection, rend la notification des incidents de confidentialité obligatoire et modifie les dispositions relatives à la biométrie prévues à la *Loi concernant le cadre juridique des technologies de l'information*.

7.1. Cybersécurité

En vigueur le 22 septembre 2023

Mesures de sécurité. Les obligations relatives aux mesures de sécurité prévues à l'article 10 de la LPRPSP demeurent inchangées. À titre de rappel, les entreprises doivent prendre les mesures de sécurité appropriées et raisonnables pour protéger les renseignements personnels en tenant compte, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Ainsi, plus un renseignement sera sensible, et plus les mesures de sécurité devront être robustes. Les mesures de sécurité visent entre autres les contrôles techniques, physiques et organisationnels et devraient toujours être évaluées et prédéfinies selon les circonstances propres à chaque projet, en procédant à une analyse technique des risques de sécurité en parallèle à l'EFVP. De cette manière, les organisations peuvent mettre en place les arrangements requis avant la signature du contrat en tenant compte des résultats de ces deux évaluations, lesquelles influenceront grandement les recommandations juridiques et la négociation des clauses contractuelles. L'analyse des risques de sécurité devrait toujours comprendre une vérification diligente de la posture de sécurité du fournisseur ainsi que de la solution ou du service offert, le cas échéant.

Mesures de protection. Dans le cadre des amendements apportés à la LPRPSP en matière d'EFVP, il est prévu que le responsable de la PRP puisse suggérer, à toute étape d'un projet, des « mesures de protection des renseignements personnels » (art. 3.4 (2)) applicables au projet (voir la section 2.3). Ces « mesures de protection » décrites à l'article 3.4 s'ajoutent ainsi à celles de mettre en place les mesures de sécurité appropriées prévues à l'article 10 de la LPRPSP. À tout événement, le responsable de la PRP devrait collaborer en continu avec un expert en sécurité pour assurer une cohérence dans l'identification et la mise en place des mesures de sécurité et de protection.

Gel de sécurité. Le « gel de sécurité » fait partie des mesures de protection des renseignements personnels contenus dans les dossiers des agents d'évaluation du crédit, prévues à la *Loi sur les agents d'évaluation du crédit*. Selon cette loi, le gel de sécurité interdit à l'agent d'évaluation du crédit qui détient le dossier qui en fait l'objet de communiquer les renseignements personnels qu'il contient ainsi que ceux qu'il produit à partir de ceux-ci, lorsque cette communication a pour fin la conclusion d'un contrat de crédit, l'augmentation du crédit consenti en vertu d'un tel contrat ou la conclusion d'un contrat de louage à long terme de biens ou d'un contrat à exécution successive de service fourni à distance. L'article 8.4 introduit par la Loi 64 ajoute que lorsqu'une personne est avisée du gel de

sécurité d'un dossier détenu par un agent, elle ne peut en demander communication auprès d'un autre agent d'évaluation du crédit. Ainsi, à l'interdiction de communiquer les renseignements personnels par les agents s'ajoute celle interdisant la communication auprès d'un autre agent.

Pistes de conformité

1. **Catégoriser les actifs informationnels de manière à y attribuer des mesures de sécurité correspondant au niveau de catégorisation.**
   - Les niveaux de catégorisation devraient tenir compte du niveau de sensibilité des renseignements personnels, et des besoins en confidentialité, intégrité et disponibilité.
2. **Mettre en place un système de collaboration entre le responsable de la PRP et le département de sécurité de manière à ce que les mesures de sécurité et de protection soient effectives et cohérentes d'un projet à l'autre.**
   - Au besoin, former un comité pour la PRP réunissant le responsable de la PRP, de la sécurité, de la gouvernance et des TI.
3. **Si applicable, mettre à jour les procédures afin que le personnel n'entre pas en communication avec des agents d'évaluation du crédit si un gel de sécurité a été porté à un dossier en vertu de la *Loi sur les agents d'évaluation du crédit*.**

7.2. Incidents de confidentialité

En vigueur le 22 septembre 2022

Depuis le 22 septembre, le Québec est devenu la troisième juridiction au Canada, avec le fédéral et l'Alberta à se doter d'un régime de notification obligatoire des incidents de confidentialité présentant un « risque de préjudice sérieux ». Le nouvel article 3.6 définit la notion d'incident de confidentialité comme étant l'accès, l'utilisation, la communication non autorisée, la perte de renseignements personnels ou toute autre atteinte à la protection de renseignements personnels. Cette définition étant plutôt large, toute atteinte, brèche ou incident de sécurité de touchant les renseignements personnels tombera sous l'application de l'article 3.6. Parmi les différents types d'incidents de confidentialité, on retrouve par exemple l'hameçonnage, le déploiement de logiciels malveillants, les attaques par rançongiciel, les botnets, les attaques par force brute, l'envoi de renseignements personnels à une mauvaise adresse courriel, etc.

⚠ Il est intéressant de souligner que le Québec est la seule juridiction au Canada à inclure l'utilisation non autorisée de renseignements personnels dans sa définition d'incident de confidentialité. Cette inclusion pourrait engendrer des difficultés d'interprétation, à savoir si une utilisation sans consentement à des fins marketing, par exemple, puisse être considérée comme un « incident de confidentialité ». Bien qu'une telle interprétation puisse conduire à une surabondance de notifications des incidents à la CAI et aux individus concernés, les entreprises devront faire preuve de jugement dans leur évaluation du risque de préjudice, tel qu'expliqué aux sections suivantes.

Évaluation du risque de préjudice sérieux. Tous les incidents de confidentialité devront faire l'objet d'un processus d'évaluation du « risque de préjudice sérieux », afin de déterminer si l'incident en question devra être notifié à la CAI et aux individus concernés. La notion de « risque de préjudice sérieux » proposée par le législateur québécois se distingue subtilement de celle de « risque réel de préjudice grave » prévue à la LPRPDÉ et la PIPA de l'Alberta, le terme « réel » ayant été omis. De plus, contrairement à la LPRPDÉ, la Loi 64 ne fournit pas de définition ou d'exemples de préjudice sérieux, mais énonce néanmoins les principaux facteurs à considérer pour évaluer le niveau de gravité du risque de préjudice :

(i) **La sensibilité des renseignements en cause.** Les renseignements qui, en raison de leur nature (ex. médicale, biométrique ou autrement intime) ou du contexte de leur utilisation, feront croître le risque de préjudice;

(ii) **Les conséquences appréhendées de leur utilisation.** Par exemple si les renseignements compromis sont susceptibles d'être utilisés pour commettre une fraude ou un vol d'identité;

(iii) **La probabilité qu'ils soient utilisés à des fins préjudiciables.** Si, par exemple, les renseignements ont été exfiltrés sur des serveurs de l'entreprise ou publiés sur le Dark Web, ils risquent d'être utilisés à de mauvaises fins (art. 3.7).

⚠ Bien que les critères d'évaluation de la LPRPDÉ et de la PIPA soient en apparence similaires avec le test formulé par la Loi 64, il se peut que la CAI interprète les obligations de notification de manière plus stricte, puisque le risque de préjudice sérieux n'aura pas à être réel pour que ce déclenche l'obligation de notification. Dans tous les cas, le responsable de la PRP devra être consulté pour effectuer cette évaluation (art. 3.7 *in fine*).

Notification des incidents. Si l'organisation détermine que l'incident présente un risque de préjudice sérieux pour les individus touchés, elle doit aviser la CAI ainsi que tout individu concerné par l'incident, à défaut de quoi la CAI pourra lui ordonner de le faire (art. 3.5 al. 2). Il est également prévu que l'entreprise peut, à sa discrétion, aviser toute personne ou organisme susceptible de réduire le risque de dommage, mais en ne lui communiquant que les renseignements personnels nécessaires à cette fin (sans le consentement de l'individu concerné). Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication. Aucun délai n'est prévu pour la notification des incidents, mais celle-ci devra se faire avec « diligence », selon l'article 3.5. À titre comparatif, la LPRPDÉ exige la notification dès que possible au CPVP dans le cas où une atteinte aux mesures de sécurité présente un « risque réel de préjudice grave ». En Europe, le RGPD exige la divulgation d'une atteinte à l'autorité de surveillance du pays au plus tard 72 heures après la violation lorsqu'elle entraîne un risque de préjudice.

Si un incident de confidentialité se produit chez un fournisseur de services tiers ou un sous-traitant à qui des renseignements personnels ont été externalisés, certaines conditions relatives à la notification des incidents devraient être prévues contractuellement. Toutefois, puisque les nouvelles obligations de notification s'appliquent à toute organisation, et ce, peu importe le rôle qui leur est attribué dans le traitement des renseignements personnels, un fournisseur de services ou un sous-traitant pourrait être tenu de signaler l'incident puisque l'obligation s'applique à « toute personne exploitant une entreprise qui a des motifs de croire que s'est produit un incident de confidentialité impliquant des renseignements personnels qu'elle détient ». Au niveau fédéral, la LPRPDE stipule qu'une organisation

doit signaler au CPVP « toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion ». Il n'est pas clair si le législateur québécois a volontairement omis de mentionner la notion de contrôle (i.e. « dont elle a la gestion ») et si la CAI s'attend à ce que tant l'organisation agissant en tant que responsable du traitement des données que son fournisseur de services (et sous-traitant) signale l'incident, ce qui pourrait nécessiter une certaine coordination entre l'organisation et son fournisseur de services.

Malgré qui précède, soulignons qu'un individu concerné par un incident de confidentialité n'a pas à être avisé si un tel avis serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, selon l'article 3.5.

Avis à la CAI. En vertu du nouveau *Règlement sur les incidents de confidentialité*, les renseignements suivants doivent être notifiés à la CAI lorsque l'organisation constate qu'un incident de confidentialité présentant un risque de préjudice sérieux a eu lieu:

1. le nom de l'organisation ayant fait l'objet de l'incident de confidentialité et, le cas échéant, le numéro d'entreprise du Québec qui lui est attribué en vertu de la *Loi sur la publicité légale des entreprises* (chapitre P-44.1);
2. le nom et les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident;
3. une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
4. une brève description des circonstances de l'incident et, si elle est connue, sa cause;
5. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
6. la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
7. le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;
8. une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
9. les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, en application du deuxième alinéa de l'article 3.5 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, de même que la date où les personnes ont été avisés ou le délai d'exécution envisagé;
10. les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à

atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé;

11. le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

    Il est à noter que la CAI a publié sur son site Internet un formulaire d'avis pour signaler un incident de confidentialité. Toutefois, ce formulaire semble requérir plus d'informations que ce que le *Règlement sur les incidents de confidentialité* exige.

Avis aux personnes concernées. Le *Règlement sur les incidents de confidentialité* prévoit que la notification aux personnes concernées par un risque de préjudice sérieux à la suite d'un incident de confidentialité doit contenir :

1. une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
2. une brève description des circonstances de l'incident;
3. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
4. une brève description des mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
5. les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
6. les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

Mitigation des risques. L'article 3.5 oblige les entreprises ayant des « motifs de croire » qu'un incident de confidentialité a eu lieu de prendre des « mesures raisonnables pour diminuer le risque qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ». Cette exigence s'applique à toute entité ou tiers assurant la garde ou l'hébergement des renseignements personnels, tel qu'un fournisseur de service ou un sous-traitant. En pratique, cela signifie que les organisations doivent prendre toutes les mesures appropriées et raisonnables afin de prévenir le préjudice pouvant être causé aux individus à la suite de l'incident et ce, même si l'incident ne présente pas de risque de préjudice sérieux. Les mesures à prendre doivent être déterminées en fonction du type d'incident et du contexte applicable, mais peuvent inclure par exemple des enquêtes approfondies et toute mesure de sécurité visant à contenir et à éradiquer l'incident.

Une bonne façon de prévenir les incidents et les risques de dommage est de doter d'un programme de sécurité robuste basé sur les bonnes pratiques de l'industrie, et de faire tester son plan de réponse aux incidents par un spécialiste de la gestion des incidents.

Registre des incidents. Les entreprises doivent tenir un registre des incidents de confidentialité, qui doit contenir les renseignements suivants :

1. une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
2. une brève description des circonstances de l'incident;
3. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
4. la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
5. le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
6. une description des éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
7. si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;
8. une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.

Pouvoirs de la CAI. La CAI dispose de plusieurs pouvoirs d'ordonnance en lien avec les incidents de confidentialité. Elle peut notamment ordonner à toute personne d'appliquer les mesures jugées pertinentes afin de protéger les droits des personnes concernées.

Pistes de conformité

1. **Définir une structure organisationnelle prévoyant des rôles et responsabilités clairs en matière de prévention, de gestion et de réponse aux incidents.**
    - Les responsabilités devraient être détaillées et précises en fonction des rôles.

2. **Élaborer et le cas échéant mettre à jour la politique de gestion des incidents de l'entreprise de manière à y inclure les nouvelles obligations, et**
    - Élaborer un plan de réponse aux incidents détaillé et basé sur les standards de l'industrie;
    - Faire tester et approuver ce plan par des experts en réponse aux incidents.

3. **Réviser les contrats avec des fournisseurs de service afin d'y inclure les nouvelles obligations de notification des incidents de manière à s'assurer que :**
    - Tous les incidents impliquant des renseignements personnels sont communiqués à l'entreprise rapidement;
    - Les clauses reflètent la nouvelle définition d'un incident de confidentialité;
    - Le fournisseur est en mesure de communiquer à l'entreprise toutes les informations requises pour lui permettre d'évaluer le risque de préjudice sérieux.

4. **Définir un programme de formation en matière de prévention et de gestion des incidents.**

5. **Tenir un registre au sein de l'entreprise de tous les incidents de confidentialité et ce, même s'ils ne comportent pas de risque de préjudice sérieux.** Ce registre devrait comprendre au minimum :
    - Le responsable de l'enquête;
    - Les circonstances de l'incident;
    - La date ou la période où il y a eu un incident;
    - La nature des renseignements personnels visés par l'incident, pour autant qu'elle soit connue;
    - La raison pour laquelle l'entreprise juge que l'incident ne comporte pas de préjudice sérieux pour les individus concernés.

7.3. Biométrie

En vigueur le 22 septembre 2022

La biométrie (qui signifie littéralement « mesure du corps humain », en grec) est une pratique qui permet l'analyse mathématique des caractéristiques biologiques, morphologiques ou comportementales d'une personne. Lorsque nous parlons de biométrie au sens de la LCCJTI, nous nous rapportons aux systèmes déployés pour identifier ou confirmer l'identité d'une personne en utilisant ses données biométriques, telles que les empreintes digitales, la structure de l'iris ou de la rétine, la géométrie de la main ou du visage, ou la voix. Il s'agit d'une nuance importante, puisque les données biométriques sont considérées comme des renseignements personnels sensibles et que ces derniers sont assujettis aux lois sur la protection des renseignements personnels applicables aux secteurs public et privé et ce, quel que soit le but pour lequel elles sont employées.

L'identification et l'authentification sont les principales fonctions de la biométrie. Chacune de ces fonctions dispose de composantes techniques qui lui sont propres, générant ainsi des risques juridiques distincts. Alors que la notion d'« identification » signifie de trouver une identité dans une base de données pour déterminer qui est une certaine personne, la notion d'« authentification » consiste plutôt à vérifier ou à confirmer l'identité de cette personne. Par exemple, l'identification peut être utilisée pour autoriser ou refuser un accès (c'est-à-dire que la présence des données biométriques capturées a été confirmée dans la base de données), alors que l'authentification permet plutôt de vérifier ou de confirmer que l'individu est bien celui qu'il prétend être. La fonction d'identification soulève généralement plus de risques techniques et juridiques puisqu'une base de données biométriques doit être instaurée, ce qui n'est pas nécessairement le cas pour la fonction d'authentification.

Le législateur québécois avait prévu, depuis 2001 avec la LCCJTI quelques dispositions visant à encadrer l'utilisation des bases de données biométriques afin d'en assurer une certaine sécurité. La Loi 64 apporte certains changements aux articles 44 et 45 de cette loi, plus particulièrement concernant l'obligation de déclarer l'utilisation des technologies biométriques à la CAI. Jusqu'à présent, cette obligation se limitait aux « banques de caractéristiques ou de mesures biométriques » (en d'autres mots, aux bases de données biométriques). Maintenant, à l'obligation d'obtenir le consentement exprès des individus pour la collecte de leurs données biométriques prévue à l'article 44 s'ajoute celle d'avoir préalablement divulgué à la CAI l'utilisation de procédés ou systèmes biométriques destinés à la vérification ou à la confirmation de l'identité et ce, sans égard à l'existence d'une base de données biométriques. Ainsi, sans une telle déclaration à la CAI et le consentement exprès, nul ne pourra faire usage de technologies biométriques pour les fins ci-haut mentionnées. Cette nouvelle exigence est cohérente avec les recommandations de la CAI concernant la Loi 64 dans son document intitulé « Mémoire de la Commission d'accès à l'information présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques ». La CAI a publié sur son site Internet un formulaire pour déclarer l'utilisation d'un système biométrique. Il est à noter que le même formulaire est utilisé pour la déclaration d'un système biométrique et d'une banque de caractéristiques ou de mesures biométriques.

Soulignons ici qu'une différence de langage entre les versions anglaise et française de l'article 44 peut mener à deux interprétations complétement différentes de cette nouvelle obligation. Alors que la version française prévoit que « Nul ne peut exiger, sans l'avoir divulgué préalablement à la Commission d'accès à l'information et sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques », la version anglaise se lit comme suit : « A person's identity may not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the person concerned ». Ainsi, la version française s'interprète *a contrario* comme nécessitant d'exiger l'utilisation de la biométrie pour que l'obligation de déclarer le système s'applique. Or, puisqu'il n'est pas possible au Québec d'exiger une telle initiative, l'amendement apporté à l'article 44 pourrait tout simplement ne pas trouver application. Ainsi, il est probable que la CAI se fie à la version anglaise de l'article 44 et oblige toute organisation traitant des données biométriques à lui déclarer et ce, même si l'organisation ne l'exige pas.

Pour finir, il est à noter que l'article 45 de la LCCJTI a été modifié de manière à obliger les organisations à déclarer à la CAI toute création de base de données biométriques au plus tard 60 jours avant sa mise en service. La LPRPSP prévoit ainsi un délai maximal pour cette divulgation préalable.

Pistes de conformité

1. **Mettre en place une directive sur l'utilisation de systèmes biométriques** de manière à y prévoir les obligations ci-haut mentionnées.
2. **Faire une évaluation des facteurs relatifs à la vie privée** préalablement à tout projet impliquant des données biométriques.

Le présent Guide sera mis à jour régulièrement par l'équipe Respect de la vie privée et protection des renseignements personnels de BLG (Montréal) afin de refléter les développements réglementaires et les lignes directrices publiées par la CAI et les autres intervenants.

Principaux contacts

Pour toute question sur les récents développements concernant le cadre juridique régissant la protection des renseignements personnels au Québec, veuillez communiquer avec l'un des membres de l'équipe Respect de la vie privée et protection des renseignements personnels de BLG :

Katherine Poirier
Associée
T 514.954.3175
kpoirier@blg.com

Frédéric Wilson
Avocat-conseil
T 514.954.2509
fwilson@blg.com

Julie Gauthier
Avocate-conseil
T 514.954.2555
jugauthier@blg.com

Patrick Laverty-Lavoie
Avocat principal
T 514.395.3887
plavertylavoie@blg.com

Candice Hévin
Avocat principal
T 514.954.2588
chevin@blg.com

Simon Du Perron
Avocat
T 514.954.2542
sduperron@blg.com

Andy Nagy
Avocat
T 514.395.2714
anagy@blg.com

Catherine Labasi-Sammartino
Avocate
T 514.954.2357
clabasisammartino@blg.com