mccarthy tétrault

Protection des renseignements personnels du Québec Trousse de mise en conformité

Explorer le nouveau régime de la Loi 25 (anciennement le projet de loi nº 64)

mccarthy tétrault

Le présent article ne contient que de l'information générale et n'est pas destiné à fournir des conseils juridiques

Trousse de mise en conformité à la Loi 25

1 Introduction

Le 22 septembre 2021, la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (« Loi 25 », anciennement appelée le projet de loi nº 64) a reçu la sanction royale.

L'adoption de la Loi 25 a remanié en profondeur le régime de protection des renseignements personnels du Québec et aura des conséquences majeures pour les entreprises faisant affaire dans cette province ou traitant les renseignements personnels des résidents du Québec. Visant à promouvoir la transparence et à améliorer la protection des renseignements personnels, les principaux changements apportés à la Loi sur la protection des renseignements personnels dans le secteur privé, telle que modifiée par la Loi 25 (collectivement, la « Loi sur le secteur privé ») comprennent des obligations plus strictes pour les entreprises, une responsabilité accrue et des sanctions plus lourdes en cas de non-conformité.

Alors, qu'est-ce que cela signifie pour votre entreprise? Pour s'assurer d'être conforme, il faut effectuer une planification attentive et avoir une compréhension approfondie de cette approche propre au Québec de la protection des renseignements personnels. La Loi 25 obligera les entreprises à passer en revue leurs pratiques et processus liés à la collecte et à l'utilisation des renseignements personnels. Bon nombre de pratiques actuelles ne seront pas conformes aux nouvelles exigences introduites par la Loi 25, et les entreprises devront s'ajuster en conséquence. La Loi 25 a créé de nouvelles sanctions en cas de non-conformité, y compris des sanctions pécuniaires massives.

La présente trousse a été conçue pour vous aider à vous conformer à la Loi 25. Elle aidera votre entreprise à comprendre la nouvelle couche de réglementation qui a été ajoutée par la Loi 25 aux obligations fédérales et provinciales antérieures. Plus que jamais, les entreprises doivent maîtriser le cadre législatif et réglementaire entourant les renseignements personnels. Cette trousse vous aidera, vous et votre entreprise, à tracer votre parcours de mise en conformité.

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

Septembre 2022 : nouvelles obligations

- ✓ Nomination d'un responsable de la protection de la vie privée
- ✓ Signalement des atteintes à la protection des données
- ✓ Exceptions au consentement pour :
  - Transactions commerciales;
  - Études, recherches ou productions de statistiques;
- ✓ Divulgation à la Commission d'accès à l'information des banques de données biométriques et des utilisations de la biométrie à des fins d'authentification

Septembre 2023 : nouvelles obligations

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

Septembre 2024 : nouvelles obligations

- ✓ Droit à la portabilité des données

2 Introduction de sanctions administratives pécuniaires

L'un des principaux changements introduits par la Loi 25 est l'institution d'un régime prévoyant l'imposition de sanctions administratives pécuniaires d'un montant conséquent. Ce régime sera mis en œuvre le 22 septembre 2023.

Il confère à la Commission d'accès à l'information (la « **Commission** » ou « **CAI** ») le pouvoir d'imposer des sanctions administratives pécuniaires dans le but de promouvoir l'atteinte des objectifs poursuivis par la Loi sur le secteur privé, d'encourager les entreprises à prendre les mesures requises pour remédier au manquement et de dissuader la répétition de tels manquements. La Commission se voit conférer le pouvoir d'imposer des sanctions administratives pécuniaires pour un très large éventail de manquements aux termes de l'article 90.1 de la Loi sur le secteur privé.

Le montant maximal des sanctions administratives pécuniaires imposé à une entreprise est de 10 millions de dollars ou jusqu'à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé. Ces montants sont comparables à ceux prévus par le *Règlement général sur la protection des données* (« **RGPD** ») de l'Union européenne.

La Loi 25 confère aussi à la Commission le droit d'intenter des poursuites pénales relativement à une infraction en vertu de la Loi sur le secteur privé. Ainsi, les avocats de la Commission peuvent intenter une action pénale devant la Cour du Québec comme le fait le Directeur des poursuites criminelles et pénales. Ces poursuites pénales pourraient donner lieu, pour les entreprises, à des amendes d'un montant allant de 15 000 à 25 millions de dollars ou, si elles sont plus élevées, jusqu'à 4 % du chiffre d'affaires mondial de l'exercice financier précédent.

En plus de ces importantes sanctions administratives pécuniaires, la Loi 25 prévoit aussi qu'un manquement à la Loi sur le secteur privé pourrait donner lieu à des dommages-intérêts punitifs lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde. Au Québec, la réclamation de dommages-intérêts punitifs doit être expressément prévue par un texte législatif. Ici, le législateur facilite la réclamation de dommages-intérêts punitifs par les individus ayant subi des préjudices causés par une atteinte à la Loi sur le secteur privé. Dans un tel cas, un individu peut réclamer des dommages-intérêts punitifs d'au moins 1 000 $, avec la possibilité que des réclamations individuelles se combinent dans un recours collectif.

Tableau 2 : Sommaire des sanctions pouvant être imposées aux individus et aux organisations

Sanction administrative pécuniaire (montant maximal)	Infraction pénale (montant maximal)	Dommages-intérêts civils
Pour les entreprises/sociétés : 10 000 000 $ ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent **Pour les individus :** 50 000 $	**Pour les entreprises/sociétés :** 25 000 000 $ ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent **Pour les individus :** 100 000 $	1 000 $ de dommages-intérêts au minimum

La Loi sur le secteur privé prévoit que la Commission prend la décision d'imposer une pénalité administrative pécuniaire et détermine le montant de celle-ci après évaluation de plusieurs critères, dont les suivants :

- La nature, la gravité, la durée et le caractère répétitif du manquement
- La sensibilité des renseignements personnels concernés par le manquement
- Le nombre de personnes concernées par le manquement et le risque de préjudice auquel ces personnes sont exposées
- La capacité de payer de la personne en défaut

La réponse de l'entreprise au manquement aura également une incidence importante sur l'évaluation par la Commission de la sanction appropriée. La Loi sur le secteur privé prévoit que la Commission peut aussi tenir compte des mesures prises par l'entreprise pour remédier au manquement ou en atténuer les conséquences, du degré de collaboration offert à la Commission et de la compensation déjà offerte à titre de dédommagement par l'entreprise aux personnes dont les renseignements personnels ont été compromis.

Les nouveaux pouvoirs en matière d'application de la loi dont est investie la Commission, conjugués au niveau extraordinairement élevé des sanctions administratives pécuniaires pouvant être imposées, changent fondamentalement le calcul du risque associé à la conformité aux règles de protection des renseignements personnels au Québec.

3 Gouvernance et responsabilité

La Loi 25 apporte des modifications notables en matière de gouvernance à la Loi sur le secteur privé, imposant aux entreprises de prendre certaines mesures, dont les suivantes :

a. nomination d'un « responsable de la protection des renseignements personnels » au sein de l'entreprise, tel qu'un chef de la protection de la vie privée;

b. établissement et publication de politiques et de pratiques sur la gouvernance en matière de renseignements personnels;

c. réalisation d'une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services faisant appel à des renseignements personnels;

d. établissement de procédures de réponse aux demandes fondées sur des droits présentées par des individus dont les renseignements personnels pourraient être recueillis.

A. NOMINATION D'UN RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

À compter de septembre 2022, chaque entreprise doit désigner un responsable de la protection des renseignements personnels qui aura le mandat de protéger les renseignements personnels et de veiller à la mise en œuvre et au respect de la Loi (art. 3 de la Loi sur le secteur privé). Par défaut, le responsable de la protection des renseignements personnels est la personne exerçant la plus haute autorité au sein de l'entreprise. Toutefois, il peut déléguer ces fonctions, en tout ou en partie, à toute personne, que celle-ci travaille ou non pour la société, ce qui permet aux entreprises d'impartir cette fonction à une personne spécialisée.

Le titre et les coordonnées du responsable de la protection des renseignements personnels doivent être accessibles au public soit sur le site Internet de l'entreprise, soit par tout autre moyen approprié (art. 3.1 de la Loi sur le secteur privé).

Tableau 3 : Exemples de responsabilités du responsable de la protection des renseignements personnels

Obligations/efforts liés à la conformité

- Assurer la conformité en matière de protection des renseignements personnels, de la sécurité et de la confidentialité
  - Veiller à ce que les services existants et les nouveaux services soient conformes aux obligations en matière de protection des renseignements personnels et de sécurité des données
  - S'assurer que l'organisation possède et tient à jour les formulaires de consentement, les formulaires d'autorisation, les avis d'information et les documents appropriés en matière de protection des renseignements personnels et de confidentialité qui reflètent les pratiques et les exigences actuelles au niveau tant interne que juridique
- Rendre opérationnels les efforts de mise en conformité
  - Tenir à jour ses connaissances en matière de législation sur la protection des renseignements personnels et surveiller l'évolution des technologies de l'information en matière de protection des renseignements personnels afin de veiller à ce que l'organisation s'y adapte ou s'y conforme

Collaboration au sein de l'organisation

- Travailler avec les équipes opérationnelles et la haute direction afin de s'assurer de les sensibiliser aux « pratiques exemplaires » sur les questions liées à la protection des renseignements personnels et à la sécurité des données
- Collaborer à l'élaboration des politiques et procédures de protection des renseignements personnels en ligne et de cybersécurité
- Travailler en collaboration avec les unités pertinentes de l'organisation pour superviser les droits d'accès à l'information des consommateurs
- Assurer la liaison en ce qui concerne la protection des renseignements personnels

Intervention en cas d'incident

- Atténuer les effets d'une utilisation ou d'une divulgation de renseignements personnels sans autorisation par les employés ou les partenaires d'affaires
- Administrer les mesures portant sur toute plainte au sujet des politiques et procédures de protection des renseignements personnels de l'organisation en coordination et en collaboration avec les autres fonctions similaires et, au besoin, les conseillers juridiques

Formation des employés

- Organiser en continu des activités de formation et de sensibilisation sur la protection des renseignements personnels

Gouvernance des données

- Veiller à ce que le recours aux technologies ait pour effet de maintenir, et non d'éroder, les mesures de protection s'appliquant à l'utilisation, la collecte et la divulgation des renseignements personnels
- Effectuer des évaluations du caractère adéquat afin de s'assurer que toute communication de renseignements personnels à l'extérieur du Québec offre une protection adéquate des renseignements personnels visés
- Mener périodiquement des évaluations des facteurs relatifs à la vie privée et, en continu, des activités de surveillance de la conformité
- Tenir compte des demandes individuelles de communication ou de divulgation de renseignements personnels ou protégés et administrer ces demandes

Contrats avec des tiers

- Élaborer et gérer des procédures d'approbation et de vérification de la conformité des fournisseurs aux politiques et aux exigences légales en matière de protection des renseignements personnels et de sécurité des données
- Veiller à ce que les accords écrits conclus avec des fournisseurs de services de traitement des données répondent de façon appropriée aux risques répertoriés lors des évaluations des facteurs relatifs à la vie privée
- Collaborer avec le conseiller juridique relativement aux contrats avec les partenaires commerciaux

Élaboration et amélioration du programme de protection des renseignements personnels

- Élaborer et coordonner un cadre de gestion des risques et de conformité en matière de protection des renseignements personnels
- Élaborer et gérer des procédures à l'échelle de l'entreprise faisant en sorte que l'élaboration de nouveaux produits et services soit conforme aux politiques et aux obligations légales en matière de protection des renseignements personnels
- Établir un processus de réception, de documentation, d'enquête et de prise des mesures nécessaires relativement à toute plainte concernant les politiques et les procédures de l'organisation en matière de protection des renseignements personnels
- Diriger la planification, la conception et l'évaluation des projets portant sur la protection des renseignements personnels et la sécurité des données
- Établir un programme interne de vérification de la protection des renseignements personnels
- Réviser périodiquement le programme de protection des renseignements personnels à la lumière des changements apportés aux lois, aux règlements ou aux politiques de l'entreprise

B. PUBLICATION DE POLITIQUES ET DE PRATIQUES DE GOUVERNANCE À L'ÉGARD DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les entreprises devront désormais tenir à jour des politiques et pratiques visant à protéger les renseignements personnels qui soient proportionnées à la nature et à la portée de leurs activités. Ces politiques doivent être rédigées en termes simples et clairs et être publiées par des moyens appropriés par l'entreprise, y compris sur son site Internet. Certaines exigences de base qui devront être abordées dans une politique de gouvernance sont les suivantes :

- un encadrement pour la conservation et la destruction des renseignements personnels;
  - aux termes de l'article 23 de la Loi sur le secteur privé, une entreprise doit détruire ou anonymiser les renseignements personnels lorsque les fins auxquelles ils ont été recueillis ou utilisés sont accomplies.
- des rôles et des responsabilités définis des membres du personnel tout au long du cycle de vie des renseignements personnels;
- un processus de traitement des plaintes concernant la protection des renseignements personnels détenus; et
- une obligation de publier sur leur site Internet leur politique de protection des renseignements personnels et ses modifications subséquentes.

C. ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Il existe deux circonstances différentes dans lesquelles la Loi 25 impose l'obligation d'effectuer une évaluation des facteurs relatifs à la vie privée.

Premièrement, la Loi 25 fait obligation aux entreprises de procéder à une évaluation des facteurs relatifs à la vie privée dans tout projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services faisant appel à des renseignements personnels (art. 3.3 de la Loi sur le secteur privé).

La réalisation d'une évaluation des facteurs relatifs à la vie privée 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.

De plus, le projet doit être de nature à permettre la portabilité des données, c'est-à-dire le droit d'un individu de recevoir l'information dans « un format technologique structuré et communément utilisé » (se reporter à la section « 4 (d) — Demandes fondées sur des droits »).

Le responsable de la protection des renseignements personnels peut, à n'importe quelle étape d'un tel projet, suggérer la mise en œuvre de mesures de protection des renseignements personnels pour contribuer à atténuer tout risque identifié.

Deuxièmement, la Loi 25 institue l'obligation de procéder à une évaluation des facteurs relatifs à la vie privée avant que puisse être communiqué à l'extérieur du Québec un renseignement personnel (art. 17 de la Loi sur le secteur privé). Cette obligation s'applique vraisemblablement aux communications tant interprovinciales que transfrontières.

L'évaluation des facteurs relatifs à la vie privée doit comprendre au moins une évaluation des éléments suivants :

i. la sensibilité des renseignements;

ii. les fins auxquelles les renseignements seront utilisés;

iii. les mesures de protection, y compris les mesures contractuelles, qui s'appliqueraient;

iv. le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.

L'information peut être communiquée si l'évaluation établit qu'elle bénéficierait d'une **protection adéquate**[1] au regard des principes de protection des renseignements personnels généralement reconnus. La communication de l'information doit faire l'objet d'une entente écrite tenant compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

Cette incertitude s'applique également lorsque la personne qui exploite une entreprise confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement.

[1]L'évaluation du seuil de « protection adéquate » est semée d'embûches. Les entreprises doivent déterminer elles-mêmes si les renseignements bénéficieraient d'une « protection adéquate ».

Par exemple, on ne sait pas exactement ce que sont les « principes de protection des renseignements personnels généralement reconnus ». S'agit-il des lois du Canada, de l'Union européenne ou d'un autre pays? Serait-il suffisant de se conformer aux Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel? La conformité aux normes en matière de vie privée intégrées aux accords commerciaux comme le traitement automatisé des données à caractère personnel du Conseil de l'Europe, serait-elle acceptable?

À ce sujet, il est important de noter que la Loi 25 n'adopte aucun des concepts du RGPD, tels que les clauses contractuelles types, les réglementations d'entreprise contraignantes, un moyen pour la Province de rendre des conclusions sur la pertinence, ou encore les mécanismes formels de sphère de sécurité.

La Loi 25 oblige les entreprises à atténuer certains risques par le biais de contrôles contractuels. Toutefois, les attentes de la Commission au sujet du niveau d'atténuation par voie de contrôles techniques, administratifs ou physiques ne sont pas claires.

D. DEMANDES FONDÉES SUR DES DROITS

Les entreprises devraient développer des processus pour faciliter leurs réponses aux demandes fondées sur les droits, mises en place par la Loi 25. À ce titre, elles devraient notamment rédiger des politiques et élaborer des procédures pour répondre en temps utile aux demandes d'accès, de rectification, de désindexation, de réindexation, de cessation de diffusion et de portabilité des données.

i. Droit d'accès et de rectification

En vertu de la Loi 25, une entreprise qui recueille des renseignements personnels doit, lors de leur collecte et par la suite sur demande, informer la personne concernée de ses droits d'accès et de rectification. Un individu peut demander la rectification d'un de ses renseignements personnels s'il est « inexact, incomplet ou équivoque » (art. 28) ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi. Compte tenu de cette exigence, les entreprises ont tout intérêt à réviser leurs politiques internes et externes en matière de vie privée afin d'informer les individus de leur droit d'accès et de rectification des renseignements personnels que l'entreprise détient à leur sujet.

ii. Droit de contrôler la diffusion des renseignements personnels

À partir du 22 septembre 2023, les individus auront le droit de contrôler la diffusion de leurs renseignements personnels par les entreprises. Ils pourront demander la cessation de la diffusion de leurs renseignements personnels ou la désindexation de tout hyperlien donnant accès à ces renseignements si la diffusion contrevient à la loi ou à une ordonnance judiciaire, ou leur cause un préjudice grave relatif au droit au respect de leur réputation ou de leur vie privée. En conséquence, les entreprises devraient mettre en place des processus pour les aider à déterminer si la diffusion continue des renseignements risque de causer un préjudice, si ce préjudice l'emporte sur le droit du public à l'information et la liberté d'expression de la personne qui publie ces renseignements, et si la mesure de réparation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice. Pour effectuer cette évaluation, l'entreprise doit tenir compte de plusieurs facteurs prescrits, dont les suivants : le statut de personnalité publique de la personne concernée; le fait que le renseignement personnel concerne une personne mineure; l'exactitude et le caractère sensible du renseignement personnel; le contexte de sa diffusion; le temps écoulé depuis sa diffusion; enfin, le fait que le renseignement soit lié à une affaire criminelle, l'obtention d'un pardon ou l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires.

Procédure relative au droit d'accès et de rectification et au droit de contrôler la diffusion des renseignements personnels :

1. **Les entreprises ne devront prendre en compte que les demandes faites par écrit par une personne qui établit que les renseignements personnels visés la concernent.**

2. **Toutes les demandes doivent être présentées au responsable de la protection des renseignements personnels. Si la demande n'est pas assez précise, le responsable de la protection des renseignements personnels doit apporter son aide pour repérer les renseignements recherchés.**

3. **Le responsable de la protection des renseignements personnels doit répondre par écrit à la demande au plus tard dans les 30 jours de la réception de la demande (art. 32). Toutefois, l'entreprise peut demander à la Commission, à l'intérieur de cette période initiale de 30 jours, de prolonger le délai dans lequel elle doit répondre (art. 46).**

4. **Si la demande est refusée, le responsable de la protection des renseignements personnels doit motiver ce refus et indiquer la disposition de la loi sur laquelle ce refus s'appuie, les recours qui s'offrent au requérant et le délai dans lequel ils peuvent être exercés. Si le requérant en fait la demande, le responsable doit également l'aider à comprendre le refus (art. 34).**

5. **L'entreprise doit informer le requérant de son droit de soumettre à la Commission une demande d'examen de mésentente dans les 30 jours du refus de la demande (art. 43).**

6. **La Commission a le pouvoir de prescrire toute mesure particulière à laquelle l'entreprise devra se conformer dans les 30 jours.**

iii. Droit à la portabilité des données

La Loi sur le secteur privé vient par ailleurs élargir le droit d'accès en accordant aussi aux individus le droit d'obtenir copie des renseignements personnels informatisés recueillis auprès d'eux. Les renseignements doivent être dans un format technologique structuré et couramment utilisé et être communiqués sous la forme d'une transcription écrite et intelligible. Les individus peuvent demander à ce que ces renseignements soient transférés directement « à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement » (art. 27 de la Loi sur le secteur privé). Les entreprises sont exemptées de répondre à une demande de portabilité des données si celle-ci « soulève des difficultés pratiques sérieuses » (art. 27 de la Loi sur le secteur privé).

Les entreprises ont jusqu'à septembre 2024 pour élaborer et mettre en œuvre un processus pour l'exportation des renseignements personnels recueillis ou stockés par des moyens numériques et pour recevoir de telles données de la part d'une autre entreprise.

4 Consentement

Le consentement était une pierre angulaire de la version antérieure de la Loi sur le secteur privé, et ce principe est encore renforcé dans la réforme introduite par la Loi 25. Dans la nouvelle version de la Loi sur le secteur privé, les exigences applicables au consentement sont étroitement liées à celles concernant la transparence.

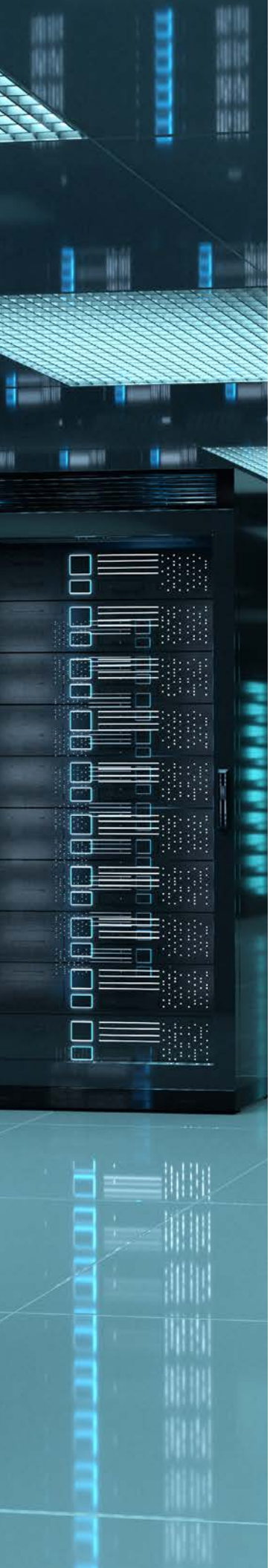
A. QUELLE INFORMATION LES ENTREPRISES DOIVENT-ELLES DONNER AUX INDIVIDUS AVANT DE RECUEILLIR DES RENSEIGNEMENTS PERSONNELS?

Avant l'adoption de la Loi 25, en vertu de la Loi sur le secteur privé, les entreprises du secteur privé devaient divulguer, avant de recueillir des renseignements personnels, l'objet de la collecte des renseignements personnels, l'utilisation des renseignements personnels, l'endroit où les renseignements personnels devaient être détenus et les droits d'accès et de rectification des renseignements personnels dont disposait la personne concernée (art. 6 de la Loi sur le secteur privé). Dans la version modifiée de la Loi sur le secteur privé, les exigences en matière de transparence ont été renforcées. Si les renseignements sont recueillis par un moyen technologique, l'entreprise doit publier sur son site Internet une politique de confidentialité et la diffuser par tout moyen propre à atteindre les personnes concernées (art. 8.2 de la Loi sur le secteur privé). Aux termes de la Loi 25, les entreprises du secteur privé doivent désormais informer les personnes de ce qui suit:

- **Les fins auxquelles ces renseignements sont recueillis** (par. 8(1) de la Loi sur le secteur privé). Les entreprises doivent en toute transparence divulguer les fins auxquelles les renseignements personnels sont recueillis.
- **Les droits d'accès et de rectification prévus par la loi** (par. 8(3) de la Loi sur le secteur privé), qui étaient déjà en vigueur dans l'ancienne version de la loi.
- **Le droit de la personne concernée de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis** (par. 8(4) de la Loi sur le secteur privé). L'octroi de ce nouveau droit ne signifie pas que les entreprises doivent réobtenir le consentement qui a déjà été obtenu avant l'adoption de la Loi 25. Si un individu a consenti à un usage en particulier de ses renseignements personnels avant l'entrée en vigueur de la Loi 25, ce consentement est toujours valable en présumant que celui-ci a été obtenu dans le respect des dispositions de la Loi antérieure alors en vigueur.
- **Le nom ou la catégorie des tiers qui auront accès aux renseignements personnels** (par. 8(2) de la Loi sur le secteur privé), par exemple si le renseignement personnel est recueilli pour le compte d'un tiers ou si la communication du renseignement personnel à des tiers est nécessaire aux fins de la collecte.
- **L'utilisation de fonctions de profilage, de localisation ou d'identification** (par. 8(2) de la Loi sur le secteur privé). Si la technologie utilisée pour recueillir des renseignements personnels utilise des fonctions de profilage, de localisation ou d'identification, les personnes concernées doivent être informées du recours à cette technologie et des moyens qui permettent de l'activer (voir l'art. 8.1 de la Loi sur le secteur privé; et section 7 – Protection des renseignements personnels dès la conception).
- Enfin, **la possibilité que le renseignement puisse être communiqué à l'extérieur du Québec** – y compris dans d'autres provinces canadiennes — doit être divulguée aux personnes concernées (art. 17 de la Loi sur le secteur privé).

La Loi 25 autorise également les individus à demander des renseignements supplémentaires. Ainsi, à la demande d'une personne concernée, les entreprises doivent divulguer :

- Les coordonnées du responsable de la protection des renseignements personnels (voir la section 3 – Gouvernance et responsabilité)
- La durée de conservation des renseignements personnels;
- La nature des renseignements personnels recueillis auprès de cette personne;
- Les catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise.
- les catégories de personnes qui ont accès à ces renseignements au sein de l'organisation.



B. COMMENT LES ENTREPRISES DEVRAIENT-ELLES PROCÉDER POUR INFORMER LES INDIVIDUS EN VUE D'OBTENIR LEUR CONSENTEMENT?

L'obligation d'obtenir le consentement directement de la personne auprès de laquelle l'entreprise recueille les renseignements personnels demeure inchangée, tout comme les exceptions correspondantes (art. 5 de la Loi sur le secteur privé). Toutefois, si l'entreprise souhaite avoir le consentement d'un mineur âgé de moins de 14 ans, elle doit l'obtenir auprès de la personne titulaire de l'autorité parentale ou du tuteur (par. 14(2) de la Loi sur le secteur privé).

En outre, les entreprises sont tenues d'utiliser un langage clair et simple dans leurs politiques de confidentialité (art. 3.2 de la Loi sur le secteur privé). De plus, lorsque la demande de consentement est faite par écrit, elle doit également être présentée distinctement de toute autre information (art. 14 de la Loi sur le secteur privé). Par conséquent, les politiques de confidentialité ne peuvent pas être intégrées à des documents plus généraux, tels que les conditions d'utilisation.

C. À QUEL MOMENT LES ENTREPRISES DOIVENT-ELLES OBTENIR UN CONSENTEMENT POUR UTILISER DES RENSEIGNEMENTS PERSONNELS?

Le principe général est que les renseignements personnels ne peuvent être utilisés qu'aux fins auxquelles ils ont été recueillis et que, si des renseignements personnels sont utilisés à l'interne par une entreprise, ils ne peuvent l'être que par les employés autorisés à qui ils sont nécessaires à l'exercice de leurs fonctions (art. 20 de la Loi sur le secteur privé). La Loi 25 ouvre la possibilité d'avoir recours au consentement implicite. L'article 12 de la Loi sur le secteur privé se lit à présent comme suit :

> *« Un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible (…) »*

Inversement, cela entraîne que le consentement à l'utilisation d'un renseignement personnel non sensible à des fins qui n'ont pas été communiquées peut être implicite plutôt qu'explicite. Néanmoins, pour être valable, le consentement doit être manifeste, libre et éclairé, et donné à des fins spécifiques (art. 14 de la Loi sur le secteur privé).

L'article 12 de la Loi sur le secteur privé prévoit également explicitement un certain nombre d'exceptions dans lesquelles l'entreprise est dispensée d'obtenir un consentement pour utiliser un renseignement personnel :

- Lorsqu'il est utilisé à des fins compatibles avec les fins auxquelles il a été recueilli, ce qui signifie qu'il a un lien pertinent et direct avec les fins auxquelles il a été recueilli;
- Lorsque son utilisation est manifestement au bénéfice de la personne concernée;
- Lorsque son utilisation est 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;
- Lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée;
- Lorsque son utilisation est nécessaire à des fins d'étude ou de recherche ou de production de statistiques et que ce renseignement est dépersonnalisé.

D. À QUEL MOMENT LES ENTREPRISES DOIVENT-ELLES OBTENIR UN CONSENTEMENT POUR COMMUNIQUER DES RENSEIGNEMENTS PERSONNELS?

La Loi sur le secteur privé prévoit que des renseignements personnels ne peuvent être communiqués que si la personne concernée y a consenti (art. 13 de la Loi sur le secteur privé). Le consentement doit être exprès lorsque ces renseignements personnels sont sensibles.

Cependant, la Loi prévoit également deux exceptions importantes à la règle du consentement à la communication d'un renseignement personnel :

- Si la communication du renseignement personnel est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise (art. 18.3 de la Loi sur le secteur privé). Pour que cette exception soit applicable, le mandat ou le contrat doit être confié par écrit, indiquer les mesures requises pour protéger le caractère confidentiel du renseignement personnel communiqué, pour que ce renseignement ne soit utilisé que dans l'exercice de ce mandat ou l'exécution de ce contrat et que la personne qui exerce le mandat ou exécute le contrat ne conserve pas le renseignement après son expiration (voir la section 5(a) – Contenu de la convention de transfert de données).
- Si la communication d'un renseignement personnel est nécessaire aux fins de la conclusion d'une transaction commerciale à laquelle une entreprise entend être partie (art. 18.4 de la Loi sur le secteur privé). Pour bénéficier de cette exception, l'entreprise doit conclure avec l'autre partie une entente stipulant : que le renseignement ne sera utilisé que pour conclure la transaction commerciale; que le renseignement ne sera pas communiqué à nouveau sans le consentement de la personne concernée; les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement; et que le renseignement sera détruit si la transaction commerciale n'est pas conclue ou si le renseignement n'est plus nécessaire pour conclure la transaction commerciale.

5 Gestion des fournisseurs

À partir de septembre 2023, la Loi 25 aura également des conséquences majeures pour les entreprises ayant des activités dans la province qui ont recours à l'impartition ou qui transigent avec des fournisseurs de services hébergeant ou traitant des renseignements personnels pour leur compte. Les conventions de services font intervenir des transferts, des communications ou des divulgations de renseignements personnels à des tiers. Les types d'ententes varient considérablement et peuvent notamment porter sur le traitement des paiements, les services de TI, les services d'intelligence artificielle (IA), l'impartition du traitement des activités et une multitude de types différents de services d'informatique en nuage. La Loi 25 viendra ajouter une nouvelle couche de réglementation venant se superposer aux lois canadiennes et internationales sur la protection de la vie privée et à d'autres régimes réglementaires devenant redondants qui s'appliquent déjà à ces transactions.

En plus d'exiger des entreprises qu'elles procèdent à des évaluations des facteurs relatifs à la vie privée avant de communiquer tout renseignement personnel d'une province à l'autre (voir section 3(c) – Évaluations des facteurs relatifs à la vie privée), la Loi 25 obligera les entreprises à revoir leurs modèles, ententes, pratiques et processus actuels. Bon nombre de formulaires standard, de modèles d'accord d'approvisionnement et d'impartition et de conventions existantes ne seront pas conformes à la Loi 25 ou imposeront aux entreprises des contraintes en matière de consentement et de transparence. Les entreprises qui ne sont pas préparées ou qui ne se conforment pas aux exigences s'exposent à des risques élevés, car la non-conformité peut donner lieu à des sanctions administratives pécuniaires très lourdes et à des droits d'action privés.

A. CONTENU DES CONVENTIONS DE TRANSFERT DE DONNÉES

Aux termes de la Loi sur le secteur privé, les entreprises sont dispensées de l'obligation d'obtenir un consentement pour divulguer des renseignements personnels à des tiers dans le contexte d'une pure convention de services. Toutefois, l'entreprise devra toujours avoir au minimum les conditions suivantes dans ses contrats avec ses fournisseurs de services :

Tableau 4 : Contenu des conventions de transfert de données

Mesures de sécurité	En vertu de l'article 10 de la Loi sur le secteur privé, toute entreprise qui communique des renseignements personnels à un fournisseur de services à des fins de traitement doit imposer des mesures de sécurité pour assurer une « protection adéquate » des renseignements personnels concernés. En vertu du principe de responsabilisation, il est conseillé d'exiger du fournisseur de services qu'il prenne des mesures de sécurité pour protéger les renseignements personnels qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.
Utilisation restreinte des renseignements	L'article 12 de la Loi sur le secteur privé restreint les utilisations des renseignements fournis à une entreprise à celles pour lesquelles un consentement a été obtenu (sauf si elles relèvent de l'une des exceptions de la liste — se reporter à la section « 4 – Consentement »). Les contrats avec les fournisseurs de services traitant des renseignements personnels doivent donc stipuler que les renseignements divulgués ne doivent être utilisés qu'aux fins de l'exécution du contrat. Cette restriction est de nature à causer des difficultés dans le cas d'un grand nombre de contrats types d'impartition qui contiennent souvent des clauses permettant au fournisseur de services d'utiliser les renseignements à d'autres fins, par exemple pour lui permettre d'améliorer la qualité de ses propres services. Elle constituera également un défi pour bon nombre d'ententes de services d'IA qui contiennent souvent des clauses permettant l'utilisation des données des clients pour l'apprentissage automatique et à des fins connexes. Compte tenu du nombre limité d'exceptions à l'exigence du consentement, les entreprises doivent évaluer attentivement quelles utilisations peuvent faire les fournisseurs de services des renseignements personnels fournis à des fins de traitement, sauf s'ils sont disposés à obtenir le consentement de leurs clients pour de telles utilisations, ou s'ils s'exposent à des risques de sanctions, d'amendes et d'actions collectives si ces consentements ne sont pas obtenus.
Destruction ou anonymisation des renseignements personnels	Les contrats passés avec les fournisseurs de services doivent inclure une clause stipulant que les renseignements qui ne sont plus nécessaires à l'exécution du mandat ne seront pas conservés. L'article 23 de la Loi sur le secteur privé donne aux entreprises le choix entre détruire un renseignement personnel et l'anonymiser pour l'utiliser « à des fins sérieuses et légitimes » lorsque les fins auxquelles le renseignement personnel a été recueilli ou utilisé sont atteintes.

Incidents de sécurité	La Loi sur le secteur privé contient des dispositions concernant les exigences en matière de notification obligatoire des incidents de confidentialité qui doivent être respectées par les entreprises et par leurs fournisseurs de services (se reporter à la section 6(b) – Gestion des incidents de cybersécurité, registre des incidents et obligation de déclarer les atteintes pour de plus amples détails). En vertu de l'article 18.3 de la Loi sur le secteur privé, le fournisseur de services doit aviser l'entreprise de toute atteinte ou tentative d'atteinte aux obligations de confidentialité. L'obligation de divulguer toute « tentative d'atteinte » sera elle aussi difficile à mettre en œuvre, car les fournisseurs de services sont généralement réticents à inclure les « tentatives d'atteinte » dans la définition des « incidents de confidentialité » devant être déclarés. Pour permettre aux entreprises de se conformer à ces exigences liées aux incidents de confidentialité, les entreprises doivent inclure des modalités de conventions de services qui obligent le fournisseur de services à : • aviser l'entreprise « sans délai 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 ». • aviser l'entreprise de tout incident de confidentialité présentant un degré de gravité suffisant et fournissant des renseignements assez détaillés pour permettre à l'entreprise de déterminer si l'incident présente un risque qu'un préjudice sérieux soit causé, auquel cas l'incident doit être notifié. La convention de services doit tenir compte des nuances précisées dans la Loi 25 quant au moment où les notifications doivent être données par l'entreprise. • « prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent » si le fournisseur de services « a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'[il] détient ». • « tenir un registre des incidents de confidentialité » et donner à l'entreprise un accès suffisant à celui-ci pour se conformer aux exigences de la Loi 25 avec l'exigence minimale que • « sur demande de la Commission, une copie de ce registre lui soit transmise ». La Loi sur la protection des renseignements personnels et les documents électroniques (« **LPRPDE** ») contient déjà une exigence similaire que, même encore aujourd'hui, certains parmi les principaux fournisseurs de services d'impartition refusent de respecter.
Droits de vérification	L'entreprise doit disposer de droits de vérification afin de pouvoir s'assurer que les mesures de sécurité requises ont été mises en œuvre par le fournisseur de services.

Autres considérations que les entreprises pourraient avoir concernant les conventions de services :

Tableau 5 : Considérations supplémentaires dans les ententes de transfert de données

Divulgation du fait que les renseignements peuvent être traités en dehors de l'entreprise	Les entreprises ne doivent pas oublier qu'en vertu de l'article 8 de la Loi sur le secteur privé, elles sont tenues d'informer les individus, lors de la collecte (et par la suite sur demande) du fait que les renseignements pourraient être divulgués à l'extérieur du Québec. Les individus doivent également être informés des noms des tiers ou des catégories de tiers auxquels les renseignements personnels seront divulgués.
Donner accès aux renseignements	La Loi 25 impose aux entreprises l'obligation de donner accès aux renseignements dans des formats particuliers (se reporter à la section 3(d)(iii) – Droit à la portabilité des données) et accorde aux individus le droit de faire rectifier les renseignements s'ils sont inexacts, incomplets ou équivoques (se reporter à la section 3(d)(i) – Droit d'accès et de rectification). Les entreprises ne doivent pas oublier d'intégrer ces obligations dans leurs conventions de services.

B. DÉCISION AUTOMATISÉE

La Loi 25 impose de nouvelles obligations aux entreprises qui utilisent les renseignements personnels pour prendre des décisions fondées exclusivement sur un traitement automatisé. L'entreprise doit informer la personne concernée du fait que la décision a été rendue exclusivement au moyen d'un traitement automatisé au moment où elle l'informe de cette décision (par. 12.1(2) de la Loi sur le secteur privé). De plus, la personne concernée a le droit de demander et de recevoir de l'information sur les renseignements personnels utilisés pour rendre la décision et les raisons, ainsi que les principaux facteurs et paramètres, qui ont mené à la décision. L'entreprise doit également divulguer à la personne concernée de l'information sur son droit de corriger les renseignements personnels utilisés pour rendre la décision.

Les entreprises qui rendent des décisions fondées exclusivement sur le traitement automatisé doivent également mettre en place un processus permettant à la personne concernée de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision.

6 Informations biométriques, cybersécurité, recherche et analyse de données

A. BIOMÉTRIE

À partir de septembre 2023, la Loi 25 crée de nouvelles obligations pour les entreprises qui utilisent des données biométriques par l'intermédiaire de certaines modifications marginales apportées aux articles 44 et 45 de la Loi concernant le cadre juridique des technologies de l'information (« **Loi sur les TI** »). Selon la définition qu'en donne le gouvernement du Québec, constitue une information biométrique toute information pouvant être utilisée pour identifier quelqu'un à partir de ses caractéristiques uniques, notamment physiques, comportementales et biologiques. Il donne des exemples de données biométriques, notamment les empreintes digitales, la reconnaissance de la forme de la main, la reconnaissance faciale et la reconnaissance vocale.

Les entreprises qui créent, utilisent ou obtiennent une banque de données biométriques doivent en informer la Commission au plus tard 60 jours après sa mise en service (art. 45 de la Loi sur les TI). De plus, l'existence d'une telle banque, qu'elle soit ou ne soit pas en service, doit aussi être divulguée à la Commission.

> **Les entreprises qui créent, utilisent ou obtiennent une banque de données biométriques doivent en informer la Commission au plus tard 60 jours après sa mise en service.**

Aux termes de la Loi 25, les données biométriques sont des renseignements sensibles. Par conséquent, tout renseignement personnel à caractère biométrique peut uniquement être recueilli par une entreprise si celle-ci obtient le consentement exprès de la personne dont les données biométriques sont recueillies (art. 44 de la Loi sur les TI).

Les entreprises doivent également divulguer à la Commission les renseignements suivants sur leur utilisation des données biométriques pour vérifier ou confirmer l'identité d'un individu avant que celui-ci ne consente à les fournir, sans égard à l'existence ou à la création éventuelle d'une banque contenant de telles données :

- les types de données biométriques recueillies
- les fins auxquelles les données biométriques seront utilisées
- les mesures de sécurité mises en place pour les protéger
- les tiers auxquels elles pourraient être communiquées
- la durée pendant laquelle elles seront conservées et les droits d'accès et de rectification de ces données dont disposent les individus
- les solutions de rechange à l'utilisation des données biométriques si l'individu ne consent pas à les communiquer.

Les entreprises doivent procéder à une évaluation des facteurs relatifs à la vie privée avant de recueillir et d'utiliser des informations biométriques (voir la section 3(c) – Évaluations des facteurs relatifs à la vie privée). Les entreprises doivent proposer des moyens d'identification de rechange si l'individu refuse de communiquer ses données biométriques. Elles doivent également limiter la collecte des données biométriques au minimum requis pour accomplir leurs fins, ne les communiquer à des tiers qu'avec le consentement de l'individu ou lorsque la loi le permet, et détruire les données biométriques lorsqu'elles ne sont plus utilisées pour identifier l'individu, ou encore si l'individu retire son consentement. Les individus conservent le droit d'accéder et de rectifier leurs données biométriques que détiennent les entreprises.

B. GESTION DES INCIDENTS DE CYBERSÉCURITÉ, REGISTRE DES INCIDENTS ET OBLIGATION DE DÉCLARER LES ATTEINTES

En plus du cadre général de gouvernance en matière de cybersécurité (se reporter à la section 3 – Gouvernance et responsabilité), la Loi 25 introduit de nouvelles exigences majeures relatives à la gestion et à la déclaration des incidents de cybersécurité. Les entreprises doivent désormais aviser avec diligence la Commission, ainsi que toute autre personne dont un renseignement personnel est concerné, de tout incident de confidentialité qui « présente un risque qu'un préjudice sérieux soit causé ».

Aux termes de la Loi 25, on entend par « incident de confidentialité » l'accès à un renseignement personnel, son utilisation ou sa communication s'ils ne sont pas autorisés par la loi, ainsi que la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement. Cette nouvelle définition s'accompagne d'une définition élargie du renseignement personnel, qui inclut à présent, aux termes de la Loi 25, tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.

La Loi 25 introduit de nouvelles exigences majeures relatives à la gestion et à la déclaration des incidents de cybersécurité.

Lorsqu'elle évalue le risque qu'un préjudice sérieux soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, l'entreprise doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

De plus, aux termes de la Loi 25, les entreprises doivent tenir un registre de tous les incidents de confidentialité de la façon prescrite par règlement, sans égard au risque de préjudice sérieux qu'ils pourraient poser.

La Loi 25 introduit également des obligations particulières en matière d'atténuation des risques et de remédiation, que l'incident de confidentialité présente ou non un risque de « préjudice sérieux », et impose ces obligations à toute personne qui a des motifs de croire que s'est produit un incident de confidentialité.

Nous notons que, le 14 décembre 2022, le Règlement sur les incidents de confidentialité (le « **Règlement de la Loi 25** ») a été publié dans la Gazette

officielle du Québec. Le Règlement de la Loi 25, qui est entré en vigueur le 29 décembre 2022, fournit aux entreprises des détails sur la teneur des nouvelles exigences en matière d'avis et de tenue de dossiers dans le contexte des incidents de confidentialité. Ci-dessous, nous décrivons la teneur de ces nouvelles obligations en matière d'avis et de tenue de dossiers, et les comparons et les mettons en opposition avec des exigences analogues édictées dans la loi fédérale et dans celle de l'Alberta.

i. Exigences existantes en vertu de la LPRPDE et de la PIPA de l'Alberta

De la même façon que les dispositions susmentionnées de la Loi 25, la LPRPDE et la *Personal Information Protection Act* de l'Alberta (« **PIPA de l'Alberta** ») font obligation aux entreprises de déclarer toute « atteinte aux mesures de sécurité » au commissaire fédéral ou à celui de l'Alberta, selon le cas, ainsi qu'à la personne intéressée, lorsque l'atteinte présente un « risque réel de préjudice grave ». De plus, les exigences de contenu en matière de déclaration des atteintes et de tenue de dossiers de la LPRPDE et de la PIPA de l'Alberta sont énoncées dans le Règlement sur les atteintes aux mesures de sécurité (« **Règlement de la LPRPDE** ») et le (« **Règlement de la PIPA de l'Alberta** »), respectivement.

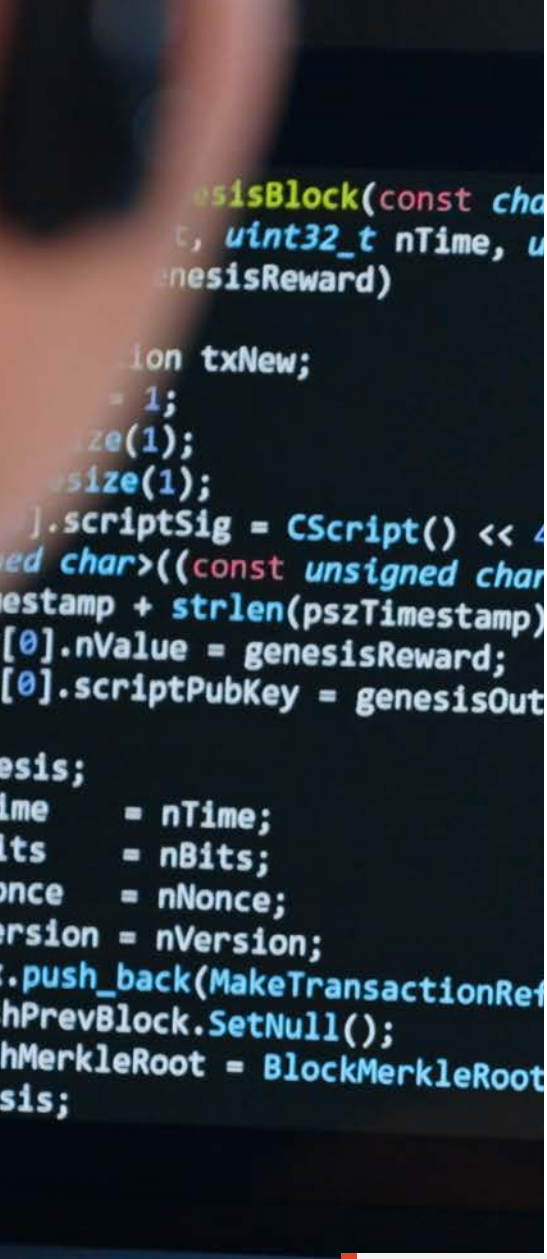
La définition que donne la Loi 25 de l'« incident de confidentialité » pourrait s'étendre à des activités allant au-delà de l'« atteinte aux mesures de sécurité » dont il est question dans la LPRPDE et dans la PIPA de l'Alberta. En outre, la nouvelle norme du « risque qu'un préjudice sérieux soit causé » applicable à la déclaration aux termes de la Loi 25 diffère de celle du « risque réel de préjudice grave » établie par la LPRPDE et par la PIPA de l'Alberta. Par conséquent, les entreprises doivent garder à l'esprit que ce libellé pourrait être interprété de façon plus stricte que la norme de la LPRPDE et de la PIPA de l'Alberta.

La définition que donne la Loi 25 de l'« incident de confidentialité » pourrait s'étendre à des activités allant au-delà de l'« atteinte aux mesures de sécurité » dont il est question dans la LPRPDE et dans la PIPA de l'Alberta.

ii. Avis à la Commission

Certains des renseignements requis que les entreprises doivent fournir à la Commission en vertu du règlement de la Loi 25 sont identiques à ceux exigés dans le Règlement sur la LPRPDE et le Règlement de la PIPA de l'Alberta. Il s'agit des suivants :

- la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- une description des renseignements personnels visés par l'incident;
- une brève description des circonstances de l'incident et, si elle est connue, sa cause;
- le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec;
- les mesures prises pour diminuer le risque de préjudice;
- les coordonnées de l'entreprise;



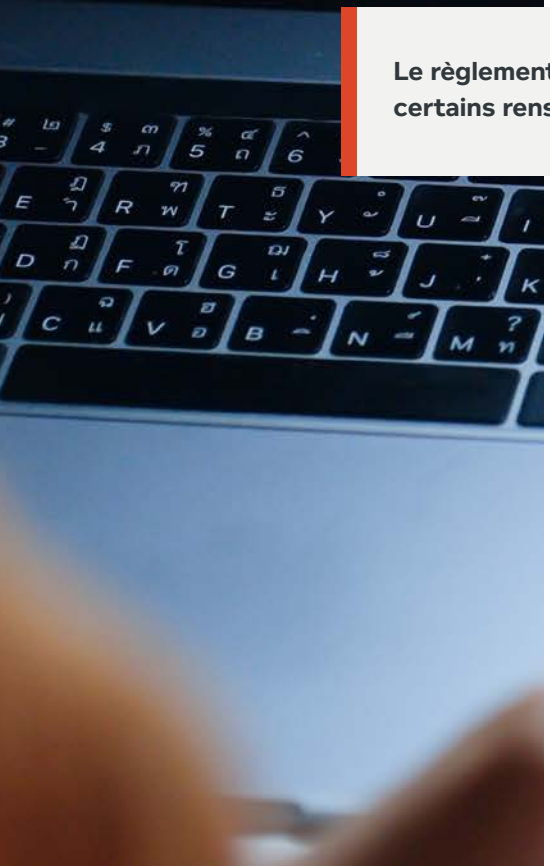
– une description des éléments ayant amené l'entreprise à conclure qu'il existait un risque de préjudice grave pour les personnes intéressées, notamment la sensibilité des renseignements personnels concernés, toute utilisation mal intentionnée possible de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité que de tels renseignements soient utilisés à des fins préjudiciables (cette obligation ne se retrouve que dans le Règlement de la PIPA de l'Alberta, quoique sous une forme moins détaillée).

Le règlement de la Loi 25 exigerait également des entreprises qu'elles fournissent certains renseignements à la Commission qui, même s'ils ne sont pas officiellement exigés en vertu du Règlement de la LPRPDE ou du Règlement de la PIPA de l'Alberta, se retrouvent cependant dans les formulaires de déclaration des atteintes recommandés par les autorités de réglementation. Il s'agit des renseignements suivants :

– la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
– la date à laquelle les personnes concernées ont été avisées, ou le délai d'exécution envisagé;
– le nom de l'entreprise;
– les mesures visant à éviter que de nouveaux incidents de même nature ne se produisent;
– le cas échéant, une mention indiquant qu'un commissaire à la protection de la vie privée à l'extérieur du Québec a été avisé de l'incident.

Le règlement de la Loi 25 introduirait plusieurs exigences en matière divulgation qui ne se retrouvent ni dans le Règlement de la LPRPDE ni dans le Règlement de la PIPA de l'Alberta. L'avis donné à la Commission doit obligatoirement contenir une explication, le cas échéant, pour laquelle il est impossible de fournir une description des renseignements personnels visés par l'incident.

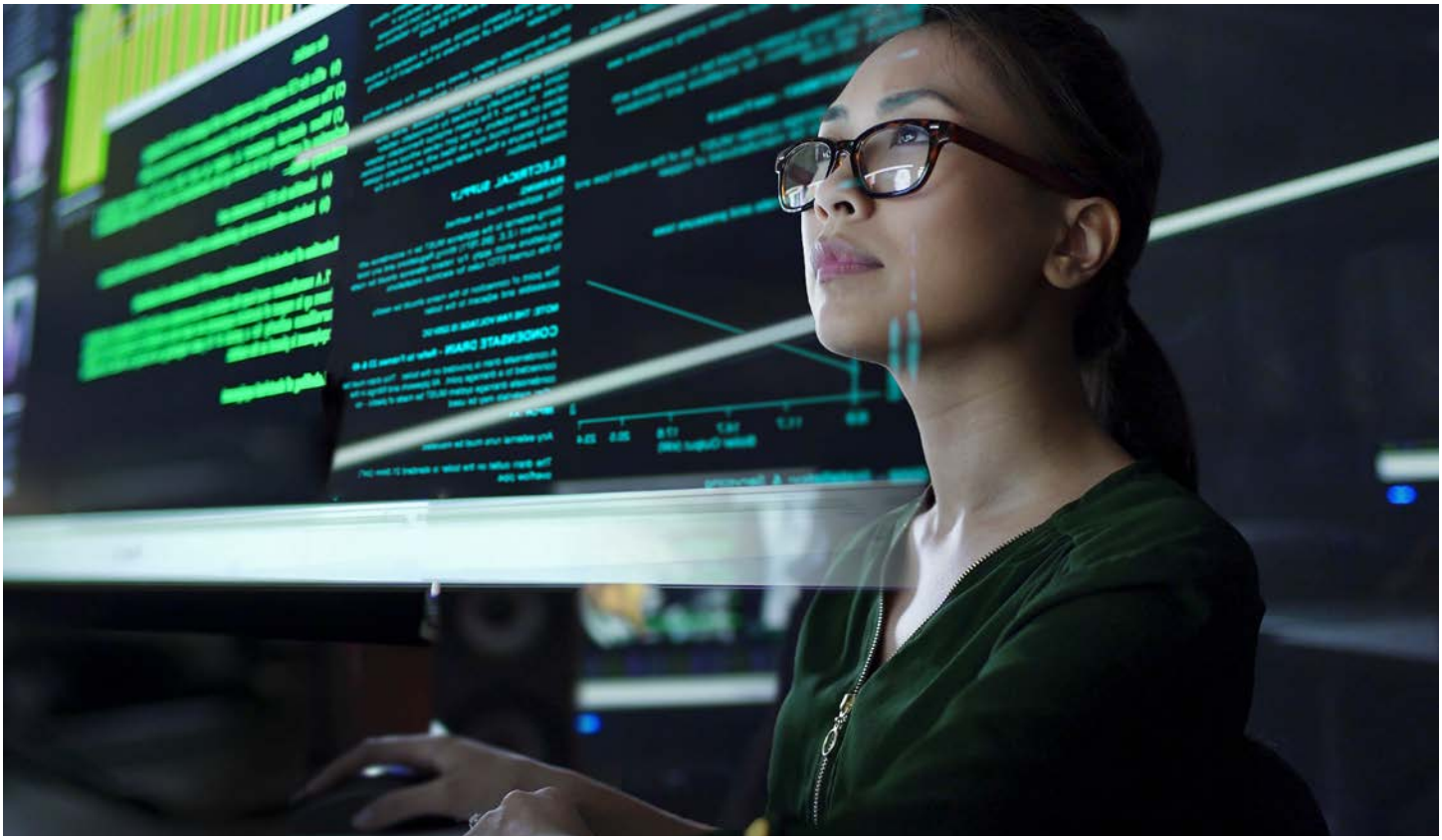
Le règlement de la Loi 25 exigerait également des entreprises qu'elles fournissent certains renseignements à la Commission.



De plus, le règlement de la Loi 25 obligerait les entreprises à tenir la Commission informée de toute information nouvelle ou supplémentaire disponible après la déclaration initiale. Le Règlement de la LPRPDE ne contient qu'une exigence de déclaration facultative de toute information supplémentaire liée à l'atteinte. Le Règlement de la PIPA de l'Alberta ne contient aucune disposition équivalente.

iii. Avis aux personnes concernées

Comme pour l'avis à la Commission, les obligations concernant les avis aux personnes concernées sont très similaires à celles des régimes de la LPRPDE et de la PIPA de l'Alberta. Aux termes du règlement de la Loi 25, les avis envoyés par les entreprises aux personnes dont un renseignement personnel est concerné par l'incident de confidentialité (si cet incident présente « un risque qu'un préjudice sérieux soit causé ») doivent indiquer la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation



de cette période; une description des renseignements personnels visés par l'incident de confidentialité; les mesures prises pour diminuer les risques de préjudice; et les coordonnées de l'entreprise. On retrouve des exigences similaires dans le Règlement de la LPRPDE et dans le Règlement de la PIPA de l'Alberta. De plus, aux termes du règlement de la Loi 25, l'avis doit comprendre une description des mesures pouvant être prises par la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice. On retrouve une obligation similaire dans le Règlement de la LPRPDE. Enfin, une exigence commune à ces trois régimes est que l'envoi d'un avis directement à la personne concernée soit la principale approche en matière d'avis, sous réserve de certaines exceptions.

Le seul élément propre au Québec en ce qui concerne les avis aux personnes concernées est l'exigence d'indiquer la raison justifiant l'impossibilité, le cas échéant, de fournir une description des renseignements personnels visés dans l'incident de confidentialité. Cette même exigence propre au Québec se retrouve dans les dispositions sur les avis envoyés à la Commission.

iv. Exigences relatives à la tenue du registre

Aux termes du règlement de la Loi 25, les entreprises doivent tenir un registre de tous les incidents de confidentialité pendant au moins cinq ans, qui doit inclure au minimum les renseignements suivants :

- la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- une description des renseignements personnels visés par l'incident;
- une brève description des circonstances de l'incident et, si elle est connue, sa cause;
- le nombre de personnes concernées par l'incident;
- les mesures prises pour diminuer le risque de préjudice;

De plus, les renseignements contenus au registre doivent être tenus à jour.

Par contre, le Règlement sur la LPRPDE exige que les dossiers soient conservés pendant 24 mois et ne précise pas leur contenu ni n'exige leur mise à jour. Quant au Règlement sur la PIPA de l'Alberta, il ne contient aucune obligation de tenue de registre.

C. RECHERCHE ET ANALYSE DES DONNÉES

La Loi 25 a apporté diverses modifications à la législation régissant l'utilisation des renseignements personnels à des fins de recherche interne, rendant ainsi les lois québécoises sur la protection des renseignements personnels plus conformes à celles des autres provinces canadiennes.

En autorisant explicitement l'utilisation de renseignements personnels anonymisés (y compris les renseignements confidentiels) sans consentement, les modifications permettent également au régime qui régit l'utilisation de renseignements personnels de bénéficier de nouvelles flexibilités importantes dans le contexte de la recherche secondaire et à des fins d'analyses de données, comme la recherche et le développement.

i. Exception au consentement pour la recherche

La Loi 25 modifie l'article 21 de la Loi sur le secteur privé et introduit les nouveaux articles 21.0.1 et 21.2.2 modernisant le processus actuel de communication de renseignements personnels à des fins de recherche dans le but d'en simplifier les mécanismes sous-jacents.

En vertu de la Loi 25, les entreprises peuvent communiquer des renseignements personnels sans le consentement des personnes concernées à un tiers qui souhaite utiliser ces renseignements à des fins d'étude ou de recherche interne ou pour la production de statistiques. Les renseignements peuvent être communiqués uniquement si une évaluation des facteurs relatifs à la vie privée conclut que :

- l'objectif de l'étude ou de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme qui permet d'identifier les personnes concernées;
- il n'est pas raisonnable d'exiger de l'organisme ou de la personne qu'il ou elle obtienne le consentement des personnes concernées, l'étude ou la recherche ou la production de statistiques l'emportant, eu égard à l'intérêt public, sur les répercussions de la communication et de l'utilisation des renseignements personnels des personnes concernées;
- les renseignements personnels sont utilisés d'une manière qui assure leur confidentialité;
- seuls les renseignements nécessaires sont communiqués au tiers.

La personne qui communique des renseignements personnels conformément à l'article 21 doit d'abord conclure une entente avec la personne ou l'organisme à qui le renseignement doit être transmis, stipulant, entre autres, que les renseignements :

- ne peuvent être accessibles qu'aux personnes qui ont besoin de les connaître pour exercer leurs fonctions et qui ont signé une entente de confidentialité;
- ne peuvent être utilisés à d'autres fins que celles précisées dans la présentation détaillée des activités de recherche et développement;
- ne peuvent être mis en correspondance avec tout autre fichier de renseignements qui n'a pas été fourni dans la présentation détaillée des activités de recherche;
- ne peuvent être communiqués, publiés ni distribués de toute autre manière que sous une forme permettant d'identifier les personnes concernées.

L'entente est envoyée à la Commission et entre en vigueur 30 jours après sa réception par la Commission.

ii. Exception au consentement pour l'analyse des données

À partir de septembre 2023, la Loi 25 modifiera l'article 12 de la Loi sur le secteur privé afin de permettre aux entreprises d'utiliser les renseignements personnels initialement recueillis à une fin précise, sans consentement, pour les utiliser au sein de la même entreprise à des fins conformes aux fins pour lesquelles ils ont été recueillis [art. 12 par. 2(1)], ainsi qu'à des fins d'étude ou de recherche ou pour la production de statistiques s'il s'agit de renseignements anonymisés [art. 12 par. 2(3)]. La Loi 25 considère qu'un renseignement est anonymisé si celui-ci ne permet plus d'identifier directement la personne concernée. Toute entreprise utilisant des renseignements anonymisés doit prendre des mesures raisonnables pour limiter le risque qu'une personne physique puisse être identifiée au moyen de renseignements anonymisés.

Nous notons que de telles initiatives de recherche interne ou d'analyse de données nécessiteraient une évaluation des facteurs relatifs à la vie privée si elles sont liées à un « projet d'acquisition, de développement et de remaniement d'un système d'information ou d'un projet de prestation de services électroniques » (art. 3.3 de la Loi sur le secteur privé).

7 Protection des renseignements personnels dès la conception

La Loi 25 renforce le principe de protection des renseignements personnels dès la conception. Premièrement, elle impose le réglage par défaut des paramètres de confidentialité liés à des produits ou des services technologiques au niveau le plus élevé de respect de confidentialité.

Les entreprises qui offrent des produits ou des services assortis de paramètres de confidentialité à plusieurs niveaux doivent veiller à ce que ces paramètres assurent par défaut le niveau le plus élevé de respect de la vie privée, de confidentialité et de protection des données. Les paramètres de confidentialité des dispositifs et des services technologiques doivent être réglés de façon à assurer le niveau de confidentialité le plus élevé. L'atteinte du niveau le plus élevé de confidentialité pour un produit ou un service ne doit nécessiter aucune intervention du consommateur, qui doit choisir lui-même tout niveau de confidentialité inférieur au niveau le plus élevé. Les technologies visées sont notamment les sites Web, les comptes de réseaux sociaux, les applications mobiles et les appareils connectés. La seule exception à cette règle concerne les témoins de connexion. Les témoins de connexion sont exclus de l'exigence de confidentialité par défaut.

Deuxièmement, la Loi 25 crée de nouvelles obligations pour les entreprises qui utilisent une technologie de profilage. Une technologie de profilage est une technologie utilisée pour recueillir des renseignements personnels permettant l'identification, la localisation ou le profilage de la personne concernée. Aux termes de la Loi 25, « le profilage 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 de la Loi sur le secteur privé).

Les entreprises qui utilisent le profilage doivent informer les individus dont les renseignements sont recueillis du recours à cette technologie. Elles doivent également informer l'individu « des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage » (art. 8.1 de la Loi sur le secteur privé). Si cette exigence est présentée comme une obligation de transparence, elle sous-entend aussi de façon plus large que les fonctions d'identification, de localisation ou de profilage d'une technologie doivent être inactives par défaut.

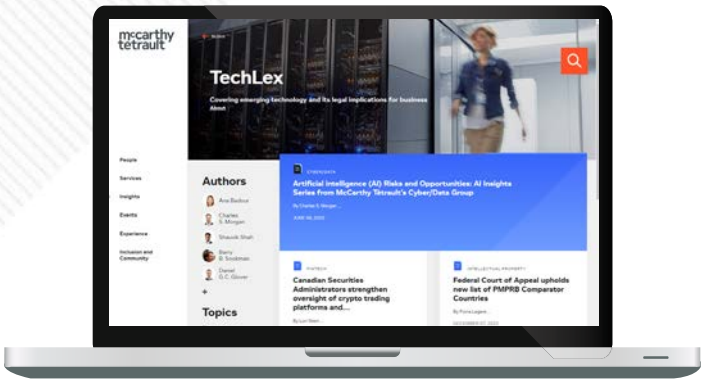
POUR OBTENIR DE PLUS AMPLES RENSEIGNEMENTS, VEUILLEZ COMMUNIQUER AVEC L'UNE DE NOS PERSONNES-RESSOURCES.

Charles Morgan
Co-Leader,
Groupe Cyber/
Données, Associé
cmorgan@mccarthy.ca
514-397-4230
MONTRÉAL

Eugen Miscoi
Associé,
Groupe Cyber/Données
emiscoi@mccarthy.ca
514-865-2393
MONTRÉAL

Dan Glover
Co-Leader,
Groupe Cyber/
Données, Associé
dglover@mccarthy.ca
416-601-806
TORONTO

Veuillez communiquer avec nous si vous avez d'autres questions à l'égard de ce qui précède. Cette trousse peut être mise à jour s'il y a lieu, au fur et à mesure de l'évolution de la réglementation et de la publication de directives pertinentes par la Commission et les autres parties prenantes.



VISITEZ NOTRE BLOGUE :

https://www.mccarthy.ca/fr/references/blogues/techlex

SUIVEZ-NOUS SUR TWITTER :

@McCarthy_ca

À propos de notre groupe Cyber/Données

Combinant une présence nationale et une approche transversale dans tous les secteurs, le groupe-conseil en protection des données et en cyberstratégie utilise une vue globale des données et de la cyberstratégie pour fournir des solutions juridiques et commerciales qui permettent d'atténuer les risques et de libérer le potentiel de création de valeur. Notre équipe pluridisciplinaire intégrée offre des conseils juridiques dans le cadre de mandats transfrontaliers, elle a conseillé des entreprises internationales lors de certains des plus grands incidents de cybersécurité et enquêtes réglementaires de l'histoire du Canada et elle influence l'état du droit canadien en matière de protection de la vie privée, de cybersécurité et de données comme aucun autre cabinet.

McCarthy Tétrault S.E.N.C.R.L., s.r.l. est un cabinet d'avocats canadien de premier plan, offrant une gamme complète de services, spécialisé dans les opérations et les litiges importants et complexes pour des clients nationaux et internationaux. Le cabinet possède des bureaux dans tous les grands centres d'affaires au Canada, ainsi qu'à New York et à Londres. Notre approche axée sur l'industrie et les compétences approfondies de notre cabinet permettent à nos clients d'obtenir des résultats commerciaux exceptionnels.

mccarthy tétrault

VANCOUVER
Suite 2400, 745 Thurlow Street
Vancouver (Colombie-Britannique) V6E 0C5

CALGARY
Suite 4000, 421 7th Avenue SW
Calgary (Alberta) T2P 4K9

TORONTO
Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto (Ontario) M5K 1E6

MONTRÉAL
Bureau MZ400
1000, rue De La Gauchetière Ouest
Montréal (Québec) H3B 0A2

QUÉBEC
500, Grande Allée Est, 9e étage
Québec (Québec) G1R 2J7

NEW YORK
55 West 46th Street, Suite 2804
New York, New York 10036
États-Unis

LONDRES
1 Angel Court, 18th Floor
London EC2R 7HJ
Royaume-Uni