COUNCIL OF CANADIAN INNOVATORS | CONSEIL CANADIEN DES INNOVATEURS

André Bachand
Président de la Commission des institutions
Édifice Pamphile-LeMay
1035, rue des Parlementaires
3e étage, Bureau 3.15

Québec, le 5 octobre 2020

Objet : Projet de loi 64 - *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*

Monsieur le Président,

Nous sommes un conseil d'affaires, fondé en 2015, qui réunit plus de 125 PDGs à travers le Canada, dont 22 au Québec, à la tête d'entreprises technologiques en expansion (scale-up) dans le secteur des technologies propres, de la cyber sécurité, des technologies financières, des technologies en santé et les technologies de l'information et de la communication. La mission du CCI est de faire entendre la voix de ces entrepreneurs dans le cadre du processus d'élaboration des politiques publiques. Tous nos membres sont des créateurs d'emploi, des investisseurs et des philanthropes implantés au Canada.

Les 20 membres du CCI au Québec, c'est un groupe dynamique de dirigeants qui gèrent des sociétés prospères dont le siège est établi au Québec. Ce sont des créateurs de richesse importants pour l'économie provinciale. Ensemble, ils maintiennent près de 6000 emplois bien rémunérés et tous s'associent à l'objectif de bâtir ici au Québec une industrie des technologies qui soit durable et locale, mais également concurrentielle à l'échelle mondiale.

La mission des entrepreneurs du CCI Québec est de faire avancer les recommandations en matière d'orientations politiques de la province, permettant ainsi aux entreprises d'innovation de renforcer leur accès aux talents, aux capitaux et aux clients de manière à solidifier leur présence et leur croissance au Québec mais également à prendre de l'expansion sur le plan international. Ils souhaitent établir un dialogue constructif avec le gouvernement pour faire en sorte que les politiques publiques québécoises en matière d'innovation ne ralentissent pas la croissance économique solide que vit le secteur des technologies au niveau provincial.

Les membres du CCI Québec salue l'initiative du gouvernement de proposer le projet de loi 64 qui tente de définir un équilibre entre la protection des données personnelles, punir adéquatement les contrevenants et maintenir un écosystème des technologies et de l'innovation robuste et durable.

PRÉAMBULE

Le présent mémorandum se destine à (i) étudier la Loi 64 adoptée à l'unanimité par l'Assemblée nationale du Québec le 12 juin 2020 – (ii) à formuler des commentaires et, le cas échéant, (iii) à proposer des amendements, le tout dans l'objectif de tenir compte du contexte mondialisé de concurrence internationale dans lequel évoluent les entreprises à forte croissance du secteur des technologies faisant affaires au Québec.

D'entrée de jeu, nous devons souligner que si la protection des renseignements personnels est un objectif légitime et louable, l'imposition de règles démesurément strictes risque d'avoir un impact majeur sur la compétitivité des entreprises québécoises à l'échelle mondiale et sur la capacité du Québec à convaincre des entreprises innovantes de se développer ou de s'installer en sol québécois.

Les entreprises membres du CCI Québec, comme tant d'autres, se conforment déjà aux normes du Règlement Général sur la protection des données européen (RGPD), et elles sont en droit de s'attendre que le projet de loi 64 ne les force pas à revoir en profondeur les processus déjà en place afin de protéger les renseignements personnels de leurs utilisateurs en conformité avec le droit étranger. Le Québec devrait se rallier aux normes internationales qui ont fait leurs preuves plutôt que de faire cavalier seul au risque de créer des obligations en contradiction avec ce qui se fait ailleurs dans le monde, au détriment des entreprises québécoises qui font affaires à l'étranger.

En ce sens, notre étude adopte une approche axée sur l'harmonisation de la législation québécoise avec les autres grands systèmes juridiques de protection de la vie privée, notamment le droit de l'Union Européenne ou encore le droit de l'État de la Californie.

Il ne s'agit pas ici d'une revue exhaustive du PL 64 mais seulement de commentaires sur des points précis qui nous semble devoir être clarifiés davantage ou bien modifiés.

Nous présentons en premier lieu une synthèse de nos recommandations, mais des commentaires supplémentaires plus détaillés sont disponibles en annexe: La *Loi sur la protection des renseignements personnels dans le secteur privé* (« **LPRPSP** ») y est reproduite et les ajouts proposés par la Loi 64 sont identifiés par un trait en surbrillance jaune.

Textes cités:

- *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5) (ci-après désignée « **LPRPDE** »)
- *Règlement (UE) 2016/679* dit « Règlement Général sur la protection des données » (ci-après désigné « **RGPD** »)
- *California Consumer Protection Act* (ci-après désignée « **CCPA** »)

SYNTHÈSE DE NOS RECOMMANDATIONS

Nous proposons que tous les termes et concepts auxquels il est fait référence dans la loi soient mieux définis et que le vocabulaire utilisé dans le PL 64 soit aligné sur les lois similaires déjà en vigueur au Canada et ailleurs afin d'éviter une confusion[1]: Les mots ont du poids dans ce genre de lois, et des nuances en apparence bénignes peuvent avoir un impact sur la portée des obligations des entreprises. Par ailleurs, l'utilisation d'un vocabulaire distinct pourrait imposer aux entreprises de réviser leurs ententes contractuelles, ce qui entraînerait des coûts supplémentaires importants. Enfin, l'adoption d'un vocabulaire décrivant des concepts juridiques déjà bien établis évitera aussi des débats sémantiques qui causeront autrement de l'incertitude au niveau contractuel.

Nous proposons les amendements suivants:

A. Items à ajouter au PL 64:

1. **Clarifier le champ d'application de la LPRPSP.** Le champ d'application de la loi à l'heure actuelle est imprécis. Une telle imprécision pourrait avoir l'effet pervers de dissuader certaines entreprises étrangères de faire affaire au Québec puisqu'elles seraient dans l'impossibilité d'évaluer si elles sont ou non soumises à la LPRPSP ce qui conduirait à un manque de prévisibilité. Il est donc important de clarifier le champ d'application de la loi, par l'introduction de critères territoriaux ou matériels déclenchant son application.

2. **Préciser les responsabilités des différents acteurs.** Il est crucial de définir et répartir les rôles et responsabilités de chacun des acteurs dans la collecte et l'utilisation de renseignements personnel. Pour cela, nous proposons de nommer:
    a. un responsable du traitement des renseignements, personne morale, qui détermine les moyens et finalités de la collecte des renseignements;
    b. un sous-traitant qui va traiter des renseignements personnels pour le compte du responsable;
    c. les éventuels sous-traitants du sous-traitant dont le rôle dans la chaîne de responsabilités doit être clairement défini;
    d. un responsable de la protection des renseignements personnels[2] avec des missions et des fonctions claires: la Loi 64 prévoit actuellement que ce poste doit être confié à un employé de l'entreprise. Nous pensons au contraire que ce poste devrait pouvoir être confié à l'externe, par exemple à un cabinet d'avocats. Les plus petites structures n'auront pas les ressources ou l'expertise pour faire porter ce chapeau à quelqu'un à l'interne. On pourrait également considérer que ce poste ne soit pas nécessaire pour les plus petites entreprises (notion de seuil à partir duquel un responsable doit être nommé).

3. **Définir les fondements légaux permettant la collecte de renseignements personnels**. Le PL 64 n'est pas claire en ce qui concerne les fondements sur lesquels une entreprise peut se baser pour collecter des données personnelles. Le consentement est l'un de ces fondements, mais il faut clarifier si celui-ci doit être exprès ou implicite. À titre d'exemple, le consentement n'est pas un fondement approprié pour les relations employeur-employé. Le PL 64 mentionne également l'intérêt légitime mais ne précise pas s'il s'agit d'un fondement alternatif à la disposition des entreprises ou bien d'une exigence supplémentaire que l'entreprise doit remplir, en plus de justifier par exemple du consentement de la personne concernée. Il serait donc important d'introduire un article qui regroupe et détaille, sur le modèle du RGPD[3], tous les fondements à la disposition d'une entreprise pour collecter des renseignements personnels: le consentement, l'intérêt légitime, l'exécution d'un contrat, une obligation légale (...).

4. **Ajouter la notion de proportionnalité et d'efforts raisonnables.** Ces deux notions devraient constituer le fil conducteur du PL 64. En effet, lorsqu'il est demandé à une entreprise de prendre des mesures pour protéger les renseignements personnels, ces mesures doivent tenir compte et être proportionnées à l'état de la technique, de la nature des données, du risque pour les individus, du coût de l'implantation. Il ne peut s'agir de mesures absolues, extraites du contexte de la collecte et de l'utilisation des renseignements personnels. De la même manière, lorsqu'une entreprise doit, en vertu du

[1] Exemples: la Loi 64 fait référence à un "risque qu'un préjudice sérieux soit causé" alors que l'on parle de "risque réel de préjudice grave" en droit canadien ; la Loi 64 évoque une "personne qui recueille des renseignements personnels": cela peut faire référence au "responsable de traitement" ou au "sous-traitant" dans le RGPD; la Loi 64 mentionne un "tiers pour qui la collecte est faite" : c'est le "responsable de traitement" du RGPD

[2] Sur le modèle du délégué à la protection des données défini dans le RGPD aux articles 37 et s.

[3] RGPD, art. 6

PL 64, accéder à une demande d'exercice des droits par exemple, elle doit déployer des efforts raisonnables en ce sens mais ne peut offrir de garanties. Il devrait donc s'agir d'une obligation de moyens et non de résultats.

B. Précisions à apporter dans le PL 64 sur:

1. **L'évaluation des facteurs relatifs à la vie privée doit être clarifiée et allégée (*Annexe page 12)*.** Bien que le dispositif soit à saluer, il est nécessaire que le projet de loi soit plus précis sur la teneur de l'évaluation demandée et le degré de formalisme requis, sous peine de conséquences négatives sur le fonctionnement des entreprises. En effet, cette analyse semble être requise dans deux situations:
    a. la mise en place d'un projet impliquant des renseignements personnels dans une entreprise. Une analyse systématique poussée aboutirait à une paralysie des projets et serait probablement impossible à mettre en place de manière effective dans des petites entreprises;
    b. la communication de renseignements personnels à l'extérieur du Québec Dans ce cas, pour une entreprise qui effectue des transferts hors du Québec de façon régulière, la lourdeur du processus pourrait ralentir considérablement les flux de données.

2. **La notion d'incident de confidentialité (*Annexe page 13*)**. L'existence d'un incident de confidentialité doit impérativement être subordonnée à la préexistence d'une violation de sécurité, à l'instar de ce qui est prévu dans les différentes lois en matière de vie privée.[4] Nous considérons que le standard de risque de préjudice sérieux proposé par le législateur québécois entraînerait des obligations démesurées pour les compagnies québécoises. Il serait utile d'uniformiser le vocabulaire avec celui du droit canadien qui parle de "risque réel de préjudice grave".

3. **La notion de consentement manifeste, libre, éclairé et donné à des fins spécifiques (*Annexe page 17*)**. Nous recommandons de clarifier que le consentement implicite énoncé au nouvel article 8.3 introduit dans le PL 64 constitue un consentement manifeste, libre, éclairé et donné à des fins spécifiques dans le cas de renseignement personnel non sensible. En effet, un consentement implicite devrait être suffisant lorsque des renseignements personnels non sensibles sont collectés pour les fins divulguées à la politique de confidentialité de l'entreprise concernée.

4. **La notion de renseignement personnel et de renseignement sensible (*Annexe page 17*)**. Le terme "renseignement personnel" étant au cœur du PL 64, nous croyons qu'il serait bénéfique de le définir clairement afin de déterminer quel type de renseignement permet d'identifier une personne physique. De même, un renseignement sensible est actuellement défini comme un renseignement qui "*suscite un haut degré d'attente raisonnable en matière de vie privée*". Cette définition repose uniquement sur des critères subjectifs. Or, au vu de l'importance des renseignements sensibles et des conséquences de cette qualification, notamment en matière de consentement, nous proposons d'introduire également dans cette définition des critères objectifs, aisément appréciables par chaque entreprise qui traite des renseignements personnels.

5. **L'anonymisation (*Annexe page 21*)**. La notion d'anonymisation mérite d'être plus développée, en détaillant notamment les mesures qui sont mises en place pour s'assurer que le renseignement a bien été anonymisé et non simplement pseudonymisé (auquel cas la ré-identification de la personne concernée est possible). Le PL 64 peut s'inspirer à cet égard du CCPA[5] qui détaille les mesures qui doivent être prises pour empêcher une telle ré-identification, ou des lignes directrices du groupe de travail de l'article 29[6].

6. **La communication de renseignements personnels à l'extérieur du Québec (*Annexe page 18*)**. Les mesures prévues dans le PL 64 préalablement à une telle communication sont en l'état actuel des choses beaucoup trop lourdes et complexes, notamment pour des PME à forte croissance qui effectuent des transferts de données de façon quotidienne et à destination de plusieurs pays dans le monde. Sous peine de ralentir considérablement les flux de données au sein d'une entreprise, il faut donc clarifier la teneur de l'évaluation des facteurs relatifs à la vie privée et son degré de formalisme et alléger le processus contractuel en tenant compte notamment des cas ou les transferts sont déjà couverts par les clauses-contractuelles types de la Commission européenne[7]. Il faut également supprimer l'exigence de prise en compte du régime juridique applicable dans l'État où ce renseignement serait communiqué, à moins que les partenaires

[4] RGPD, art. 4 ; LPRPDE art. 2 (1) ; Code Civil Californien, par. 1798.82
[5] CCPA, Article 1798.140 (h)
[6] Lignes directrices du G29 sur les techniques d'anonymisation, WP216
[7] RGPD, art. 46

commerciaux du Québec, et en premier lieu les autres provinces canadiennes[8], obtiennent immédiatement un statut d'adéquation. Cela est primordial pour la bonne continuité des affaires des entreprises québécoises, lesquelles devront sinon redoubler d'efforts et engendrer des coûts de conformité importants afin de continuer à utiliser leurs fournisseurs de services étrangers.

C. Items à supprimer dans le PL 64 de:

1. **L'obligation de publication de politiques internes sur le site internet de l'entreprise (*Annexe page 9 et 10*)**. Il faut distinguer entre les politiques externes qui visent à informer les individus des conditions entourant le traitement de leurs renseignements personnels et qui doivent être rendues publiques et les politiques internes. Les pratiques et organisations internes d'une entreprise ne devraient être communiquées que dans des conditions restreintes et strictement encadrées, et il n'est pas nécessaire, utile ou pertinent de les rendre publiques.

2. **L'obligation de prêter assistance au requérant dans le cas d'une demande de l'exercice de ses droits (*Annexe page 22*)**. Le responsable de la protection des renseignements personnels doit motiver son refus d'accéder à une demande. Cela représente une garantie suffisante que ce refus sera explicité clairement et basé sur des motifs suffisamment sérieux. L'obligation qui est faite au responsable de prêter assistance au requérant qui le demande de l'aider à comprendre le refus nous apparaît donc trop exigeante et dépourvue de valeur ajoutée.

Enfin, nous suggérons d'octroyer un délai de deux ans avant l'entrée en vigueur de la loi suite à sa sanction - au lieu du délai d'un an prévu actuellement à l'article 165 de la Loi 64 - afin de permettre aux entreprises de développer ou d'acheter des solutions de conformité et de les intégrer dans leurs opérations par défaut, ce qui permettrait par la même de rassurer les consommateurs à l'effet que leurs droits sont protégés. Étant donné les modifications substantielles à la loi présentement en vigueur, un délai d'un an rendrait difficilement réalisables ces objectifs en pratique.

En comparaison, un délai de deux ans a été octroyé en vertu du RGPD afin de permettre aux entreprises de se conformer à la celle-ci. Par ailleurs, la Chambre des Commerces des États-Unis suggère l'octroi d'un délai de dix-huit mois au lieu du délai de six mois afin de se conformer aux propositions d'amendements à la loi californienne, ce dernier étant jugé insuffisant.

Nous vous remercions de votre attention, et sommes à votre entière disposition pour discuter plus en détails de nos recommandations.

Nous vous prions d'agréer, Monsieur le Président, l'expression de notre considération respectueuse.

Benjamin Bergen
Directeur exécutif
Conseil Canadien des Innovateurs
bbergen@canadianinnovators.org

Pierre-Philippe Lortie
Directeur, Québec
Conseil Canadien des Innovateurs
plortie@canadianinnovators.org

[8] Ainsi que les États-Unis, le Royaume-Uni, le Japon ainsi que les pays membres de l'Union européenne

Dirigeants québécois et membres du Conseil canadien des innovateurs

Accedian — Patrick Ostiguy

Alayacare — Adrian Schauer

CloudOps — Ian Rae

Coveo — Louis Têtu

Cycle Capital Management — Andrée-Lise Méthot

Dialogue – Cherif Habib

District M – Jean-François Côté

EXFO — Germain Lamonde

Fiska – Patrick Huynh

GSoft – Simon De Baene

Hopper — Frédéric Lalonde

Kinova Robotics — Charles Deguire

LeddarTech – Charles Boulanger

Lightspeed — Dax Dasilva

PetalMD — Patrice Gilbert

Plusgrade – Ken Harris

Qohash - Jean Le Bouthillier

Stingray — Eric Boyko

Squeeze – Denis Doré

Stradigi AI – Basil Bouraropoulos

TrackTik – Simon Ferragne

VOTI Detection — Rory Olson

ANNEXE

I. Champ d'application de la LPRPSP

- Entreprise et renseignements

> ***Article 1.*** *La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.*
>
> *Elle s'applique à ces renseignements, que leur conservation soit assurée par l'entreprise ou par un tiers, quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles: écrite, graphique, sonore, visuelle, informatisée ou autre.*
>
> *Elle s'applique aussi aux renseignements personnels détenus par un ordre professionnel dans la mesure prévue par le Code des professions (chapitre C-26) et à ceux détenus par une entité autorisée dans la mesure prévue par la Loi électorale (chapitre E-3.3)*
>
> *Le présent projet de loi 64 ne s'applique pas à la collecte, la détention, l'utilisation ou la communication de matériel journalistique, historique ou généalogique à une fin d'information légitime du public.*
>
> *Les sections II et III du PL 64 ne s'appliquent pas à un renseignement personnel qui a un caractère public en vertu de la Loi.*
>
> *Elles ne s'appliquent pas non plus aux renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise, tel que 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.*

Commentaires :

Alinéa 1. Le PL 64 ne prévoit pas de modification à l'alinéa 1, lequel précise sommairement que la LPRPSP s'applique à une entreprise. L'exploitation d'une entreprise est définie à l'article 1525 du Code civil du Québec, qui dispose que « *Constitue l'exploitation d'une entreprise l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services* ».

Comme ni le *Code civil du Québec,* ni la LPRPSP et ni les tribunaux[9] ne viennent encadrer précisément l'application extra-territoriale de la LPRPSP, nous croyons que le PL 64 devrait corriger cette lacune. Cet aspect est primordial dans un contexte où les relations commerciales ne sont plus limitées par l'existence de frontières mais s'effectuent de manière dématérialisée.

Selon nous, la définition actuelle est floue et ne permet pas de préciser si le projet de loi entend s'appliquer également pour les activités d'une entreprise qui ne serait pas établie au Québec mais qui, en vertu d'un « faisceau d'indices », aurait des liens avec le Québec. Une telle imprécision pourrait avoir l'effet pervers de dissuader certaines entreprises étrangères de faire affaire au Québec puisqu'elles seraient dans l'impossibilité d'évaluer si elles sont ou non soumises à la LPRPSP ce qui conduirait à un manque de prévisibilité.

Le PL 64 pourrait s'inspirer de deux modèles de lois qui fixent des critères précis encadrant leur champ d'application:

[9] Antoine Guilmain et Éloïse Gratton, « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », Barreau du Québec, Service de la formation continue, *Développements récents en droit à la vie privée (2019)*, vol 465, Montréal, Yvon Blais, 2019, p. 71 et s.

- L'article 3 du Règlement Général sur la Protection des Données Personnelles (« RGPD ») dispose que:

  1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.
  2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:
  a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
  b) *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »

- De même, le *California Consumer Protection Act* (« **CCPA** ») prévoit l'introduction de deux critères matériels pour que le « business » soit soumis à l'application de la loi :

  (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

  (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

  (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

  (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

  (2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark »

Il serait judicieux que le projet de loi puisse également encadrer le type d'entreprise soumise à son application en utilisant des critères matériel et/ou territoriaux (comme par exemple le fait de traiter des renseignements personnels sur des personnes établies au Québec de manière permanente ou le fait que l'accomplissement d'activités commerciales ait lieu au Québec). À cet égard, l'approche concrète et claire proposée par le CCPA a le mérite d'établir clairement quelles entreprises sont soumises ou non à son application et, incidemment, de faciliter la conformité des entreprises identifiées à ses dispositions.

Alinéa 2. Il semble que cet ajout a vocation à préciser que la LPRPSP s'applique tant à un renseignement conservé par une entreprise au sens de la loi qu'à un renseignement conservé par un tiers. En ce sens, elle clarifie que le champ d'application de la loi est plus large que ce qui est initialement proposé.

II. Responsabilité relative à la protection des renseignements personnels

« SECTION I.1 *RESPONSABILITÉS RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

- Distinction entre entreprise et sous-traitant

Le PL 64 mentionne, à son article 18.3, l'existence de sous-traitants qui se qualifient comme « toute personne ou tout organisme ». Néanmoins, il n'existe pas de distinction formelle qui viendrait définir un sous-traitant. Il serait judicieux que la LPRPSP distingue entre l'entreprise qui contrôle les finalités et les moyens du traitement (la personne en charge) et la personne qui traite les

renseignements pour le compte de la personne en charge (le sous-traitant). Une telle distinction permettrait ainsi de bien délimiter les rôles et responsabilités de chacun des acteurs qui peuvent être impliqués dans le traitement de données au regard d'un incident de confidentialité. Par voie de conséquence, cela permettrait aussi d'allouer de manière plus équitable et cohérente les responsabilités incombant à chacun des acteurs impliqués dans le traitement.

Par exemple, le RGPD propose un modèle qui distingue entre le responsable de traitement *« qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »* et le sous-traitant *« qui traite des données à caractère personnel pour le compte du responsable du traitement »*[10]. De cette distinction découlent des obligations différentes, adaptées au rôle effectif de chacun dans le traitement des renseignements personnels.

Le CCPA introduit lui trois types d'acteurs différents: les "business", les "service provider" et les "third-party". La notion de "service provider" est similaire à celle de sous-traitant dans le RGPD: *"Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners,* ***that processes information on behalf of a business*** *and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.[11]"*

Cette qualification est fondamentale, car si une entreprise est reconnue comme étant le "service provider" d'une autre entreprise, le "business" auquel le CCPA s'applique, ce dernier sera réputé partager les données nécessaires "to perform a business purpose" et échappera alors à certaines obligations applicables lorsque le CCPA qualifie le partage de vente.

Ces deux législations mettent donc en lumière la nécessité d'une allocation claire des rôles des parties impliquées dans le traitement de renseignement personnels afin de pouvoir définir au mieux les obligations qui incombent à chacune d'entre elles.

- Responsable de la protection des renseignements personnels

> ***Article 3.1.*** *Toute personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient.*
>
> *Au sein de l'entreprise, la personne ayant la plus haute autorité veille à assurer le respect et la mise en œuvre de la présente loi. Elle exerce la fonction de responsable de la protection des renseignements personnels; elle peut déléguer cette fonction par écrit, en tout ou en partie, à un membre du personnel.*
>
> *Le titre et les coordonnées du responsable de la protection des renseignements personnels sont publiés sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendus accessibles par tout autre moyen approprié*

Commentaires :

Alinéa 1. La notion de « *personne qui exploite une entreprise* » est mentionnée à de multiples reprises dans la LPRPSP. Est-il fait référence ici à une personne morale ou à une personne physique? Ce langage prête à confusion dans la mesure où cela suggère qu'une personne physique serait potentiellement responsable juridiquement de la protection des renseignements personnels détenus par l'entreprise qu'elle exploite. Pourquoi ne pas adopter une approche simplifiée et faire référence à l'entité juridique - l'« entreprise » - qui serait responsable juridiquement d'un manquement aux obligations de la LPRPSP?

Amendement proposé : ~~*Toute personne qui exploite*~~ *Une entreprise est responsable de la protection des renseignements personnels qu'elle détient.*

[10] Article 4 du RGPD
[11] CCPA, art. 1798.140 (v).

Alinéa 2. Cet alinéa précise que le Chef de la direction sera responsable de la protection des données personnelles (« **RPRP** »). Cette responsabilité peut néanmoins être déléguée à un membre du personnel qui serait par exemple mieux à même d'endosser cette fonction.
Le langage utilisé dans la LPRPSP - « veille à assurer le respect et la mise en œuvre de la présente loi » - laisse penser qu'il existerait une potentielle responsabilité du RPRP sans pour autant le dire expressément. Il n'est ainsi pas établi si le RPRP pourrait voir sa responsabilité personnelle engagée du fait du manquement de l'entreprise aux obligations de la LPRPSP ou si cette responsabilité serait imputable à l'entreprise agissant en qualité de personne morale. Cette responsabilité doit être clairement établie et pose la question de la pertinence de rendre responsable le RPRP. Selon nous, ce dernier devrait avoir pour mission de veiller de manière indépendante à la bonne application de la LPRPSP mais ne devrait pas se voir imputer la responsabilité d'une non-conformité. Cette responsabilité devrait être imputable à l'entreprise.

Les mots ont leur importance et un langage clair a l'avantage d'effacer tout doute sur le niveau de responsabilité requis de cette fonction. Le droit de l'UE a par exemple clairement établi que le délégué à la protection des données personnelles agissait comme un conseiller du responsable de traitement et/ou du sous-traitant et que sa responsabilité personnelle ne pouvait en aucun cas être engagée. La LPRPSP mérite d'être clarifiée à cet égard.

La disposition ne nous éclaire pas davantage sur les fonctions ou les missions qui seraient déléguées à ce responsable. Cette disposition semble créer une obligation importante avec des conséquences juridiques qui doivent être clarifiées afin que les entreprises puissent pleinement anticiper les impacts et prendre des mesures appropriées à l'interne.

A cet égard, il serait judicieux de venir encadrer la fonction du RPRP en prenant exemple sur la solution qui a été retenue dans l'Union Européenne (« **U.E.** »), l'article 38 du RGPD précise ainsi que le délégué à la protection des données :

- « *doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel;*
- *doit disposer de ressources nécessaires pour exercer ces missions;*
- *ne doit pas recevoir d'instruction en lien avec l'exercice des missions;*
- *est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions;*
- *peut exercer d'autres tâches dans la mesure où cela n'entraîne pas de conflits d'intérêts* ».

De même, il est fondamental de délimiter les missions du RPRP. En effet, il est difficile d'imputer une responsabilité à un individu qui n'a pas de missions délimitées. A cet égard, exemple pourrait être pris sur l'article 39 du RGPD qui précise que les missions du délégué à la protection des données sont :

- « *informer et conseiller le responsable du traitement ou le sous-traitant en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;*
- *contrôler le respect du RGPD, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel;*
- *dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci;*
- *coopérer avec l'autorité de contrôle;*
- *faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement* ».

- Politiques internes et pratiques de gouvernance

> ***Article 3.2.*** *Toute personne qui exploite une entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels et propres à assurer la protection de ces renseignements. Celles-ci doivent notamment prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles doivent également être proportionnées à la nature et à l'importance des activités de l'entreprise et être approuvées par le responsable de la protection des renseignements personnels.*

Ces politiques sont publiées sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendues accessibles par tout autre moyen approprié.

Commentaires :

Alinéa 1. L'article 3.2 alinéa 1 a trait à l'obligation de mettre en place des politiques et des pratiques en lien avec la protection des renseignements personnels. Cette obligation est présente dans les textes internationaux sur la protection des renseignements personnels[12] et paraît essentielle. Il est en effet nécessaire qu'une compagnie mette en place tant des politiques internes que des politiques externes afin de pouvoir construire un programme de protection de la vie privée.

Néanmoins, l'article 3.2 semble mettre davantage l'emphase non pas sur les politiques externes mais sur les politiques internes de l'entreprise visant à « *prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci* ». Cela est peut-être dû au fait que l'article 8 de l'actuelle LPRPSP prévoit déjà l'obligation de mettre en place des politiques externes en disposant que :

« *La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer:*
1° de l'objet du dossier;
2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise;
3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification ».

Alinéa 2. L'obligation de publication sur le site web de l'entreprise contenue dans l'alinéa 2 suscite notre étonnement. En effet, dans quelle mesure est-ce qu'il serait nécessaire, utile ou pertinent de rendre publiques des politiques à usage interne sur le site web de l'entreprise? Cette obligation n'existe d'ailleurs pas à notre connaissance dans les grandes lois, principes et normes en matière de vie privée. Ces textes distinguent entre, d'une part, les politiques externes qui visent à informer les individus des conditions entourant le traitement de leurs renseignements personnels et qui doivent être rendues publiques et, d'autre part, les politiques internes de l'entreprise qui ont vocation à rester internes, comme leur nom l'indique[13]. La norme ISO 29100 délimite à cet égard très clairement les fonctions et finalités de ces deux types de politiques :

"*The term "privacy policy" is often used to refer to both internal and external privacy policies. An internal privacy policy documents the objectives, rules, obligations, restrictions and/or controls an organization has adopted to satisfy the privacy safeguarding requirements that are relevant to its processing of PII. An external privacy policy provides outsiders to the organization with a notice of the organization's privacy practices, as well as other relevant information such as the identity and official address of the PII controller, contact points from which PII principals might obtain additional information, etc. In the context of this framework, the term "privacy policy" is used to refer to the internal privacy policy of an organization. External privacy policies are referred to as notices[14]*".

Rendre publiquement disponible des politiques internes ayant trait aux contrôles spécifiques, aux rôles et responsabilités des équipes internes, à la mise en place de procédures pour recevoir les plaintes et les demandes de renseignements ou à l'explication interne de la mise en œuvre de ces politiques et procédures s'inscrit selon nous en porte-à-faux avec les grands principes qui sous-tendent la protection des renseignements personnels. Le premier de ces principes, qui a été énoncé notamment dans l'article 8 des lignes directrices de l'OCDE, est le principe de transparence. Ce principe sous-tend que les entreprises doivent communiquer leurs activités de traitement de renseignements personnels auprès des individus. En vertu de ce principe de transparence, il est effectivement essentiel de communiquer à l'externe la nature des renseignements collectés, les finalités de leur utilisation, l'identité de l'entreprise, les tiers avec qui les renseignements sont partagés, etc. afin notamment de permettre à ces individus d'exercer leurs droits. En revanche, les principes de garantie de sécurité, d'intégrité et de confidentialité couplés au principe de responsabilité imposent de mettre en place des politiques internes visant à garantir la protection des renseignements personnels dans l'entreprise. Ces politiques visent alors non pas à informer les individus sur leurs droits et les modalités de traitement mais à

[12] OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, principe 12; RGPD, Art. 24 (inclus dans l'obligation de mettre en place des mesures techniques et organisationnelles appropriées); PIPEDA, principe 4.1.4.
[13] Les articles 13 et 14 du RGPD précisent clairement quelles informations doivent être communiquées à l'individu à des fins de transparence. Il en va de même pour le CCPA qui précise clairement que les informations de la politique de vie privée doivent être rendues publiques (art. 1798.130 (5))
[14] ISO/IEC 29100 Information technology – Security techniques – privacy framework, 4.6.

informer et former les employés d'une entreprise sur les principes de vie privée, les spécificités des rôles attribués à chacun et sur les politiques et procédures mises en place en interne par l'entreprise pour garantir le respect de ces principes.

A ceci s'ajoute le principe général de la confidentialité des informations détenues par une entreprise qui vise à donner accès à un nombre limité de personnes, sous garanties de confidentialité, aux documents protégés par la confidentialité. Les politiques internes en matière de protection des renseignements personnels sont couverts par le sceau de la confidentialité dans toutes les entreprises. Rendre ces documents disponibles sans aucune condition à des entreprises tierces présente des risques de divulgation de pratiques et organisations internes d'une entreprise qui ne devraient être communiquées que dans des conditions restreintes et strictement encadrées.

Il est donc fortement recommandé de supprimer l'obligation de publication sur le site web de l'entreprise des politiques internes d'une entreprise en matière de protection de la vie privée.

Amendement proposé :

« 3.2. Toute personne qui exploite une entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels et propres à assurer la protection de ces renseignements. Celles-ci doivent notamment prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles doivent également être proportionnées à la nature et à l'importance des activités de l'entreprise et être approuvées par le responsable de la protection des renseignements personnels. ***Ces politiques sont publiées à l'interne*** *»*

- Évaluation des facteurs relatifs à la vie privée

> ***Article 3.3.*** *Toute personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.*
>
> *Aux fins de cette évaluation, la personne doit consulter, dès le début du projet, son responsable de la protection des renseignements personnels.*
>
> *La personne doit également s'assurer que ce projet permet qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé.*

Commentaires :

Alinéa 1. Cet article vient rendre obligatoire une analyse des facteurs de la vie privée pour tout projet de système d'information qui implique le traitement d'un renseignement personnel. Cette obligation est sous-tendue par les lois en matière de vie privée et est rendu obligatoire par le RGPD dans des cadres plus restreints[15].

Alinéa 2. L'alinéa 2 vient néanmoins apporter une lourdeur supplémentaire au processus. Une entreprise œuvrant dans le domaine des technologies de taille moyenne (entre 400 et 1000 employés) peut faire plusieurs achats d'outils technologiques par semaine. Tous ces outils, au regard de la loi devraient être analysés et soumis au responsable de la protection des renseignements personnels qui est une et même personne, ce qui paraît difficilement réalisable si cette personne est également chargée du respect de tous les autres aspects de la loi en matière de protection des données. Il nous semble donc que si l'esprit du projet de loi est la réalisation d'une véritable analyse d'impact relative à la vie privée, dans la lignée de ce qui a été mis en place par le RGPD[16], il s'agit d'une analyse trop lourde, impossible à effectuer pour tous les projets et outils mis en place par une entreprise. A contrario, s'il ne s'agit que d'une analyse très succincte et peu poussée, la portée et l'intérêt de cette évaluation est limitée. Il serait donc judicieux de venir préciser le degré de formalisme requis pour effectuer une telle analyse afin de s'assurer que les entreprises ne se retrouvent pas en violation systématique de cette section.

[15] RGPD, art. 35.
[16] RGPD, art. 35.

Alinéa 3. Cette section fait écho au droit d'accès à un renseignement personnel qui existe déjà dans la LPRPSP. Néanmoins, elle vient ajouter une obligation de fournir une copie dans un format structuré et couramment utilisé. Cela rappelle le droit à la portabilité des données prévu par le CCPA dans le cadre du droit d'accès[17] et, dans des conditions limitées, par le RGPD[18].

> ***Article 3.4.*** *Le responsable de la protection des renseignements personnels peut, à toute étape d'un projet visé à l'article 3.3, suggérer des mesures de protection des renseignements personnels applicables à ce projet, telles que :*
>
> *1° la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels;*
> *2° des mesures de protection des renseignements personnels dans tout document relatif au projet;*
> *3° une description des responsabilités des participants au projet en matière de protection des renseignements personnels;*
> *4° la tenue d'activités de formation sur la protection des renseignements personnels pour les participants au projet.*

Commentaires :

Il semble que cet article ébauche une liste de missions ou prérogatives qui sont associées au RPRP. Cette liste a cependant uniquement un caractère facultatif et ne détaille selon nous pas de manière suffisamment détaillée les fonctions ou les missions qui seraient déléguées à ce responsable (pour plus de détails, se reporter à notre commentaire de l'article 3.1)

- Incident de confidentialité

> ***Article 3.5.*** *Une personne qui exploite une entreprise et qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient doit 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 l'incident présente un risque qu'un préjudice sérieux soit causé, elle doit, avec diligence, aviser la Commission d'accès à l'information instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). Elle doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Elle peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication.*
>
> *Malgré le deuxième alinéa, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela 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.*
>
> *Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article.*

[17] CCPA, art. 1798.100.
[18] RGPD, art. 20.

Commentaires :

Cette clause est à saluer dans la mesure où elle met l'emphase sur la nécessité de notifier un incident de confidentialité.

Alinéa 1. Il serait judicieux ici de distinguer entre l'entreprise qui contrôle les finalités et les moyens du traitement (la personne en charge) et la personne qui traite les renseignements pour le compte de la personne en charge. Une telle distinction permettrait ainsi de bien délimiter les rôles et responsabilités de chacun des acteurs qui sont impliqués dans un incident de confidentialité. Par exemple, le RGPD prévoit que le responsable de traitement (la personne en charge) doit notifier les autorités de contrôle après un incident de confidentialité[19] et notifier les individus seulement si cela engendre un risque élevé pour les droits et libertés des individus[20]. Ce responsable de traitement doit lui-même être notifié par le sous-traitant.

Alinéa 2. Nous considérons que le standard de risque de préjudice sérieux proposé par le législateur québécois est hautement problématique et entraînerait des obligations démesurées pour les compagnies québécoises. Il serait utile d'uniformiser le vocabulaire avec celui du droit canadien qui parle de "risque réel de préjudice grave". Par ailleurs, le RGPD prévoit l'obligation d'aviser l'autorité gouvernementale uniquement lorsqu'il est probable que le risque se matérialise[21]. La formulation actuelle du Projet suggère que l'entreprise devrait aviser la Commission d'accès à l'information du Québec des risques théoriques et hypothétiques, ce qui crée une obligation démesurée pour les entreprises et une charge de travail impossible à supporter pour la CAI.

> ***Article 3.6****. Pour l'application de la présente loi, on entend par « incident de confidentialité » :*
>
> *1° l'accès non autorisé par la loi à un renseignement personnel;*
> *2° l'utilisation non autorisée par la loi d'un renseignement personnel;*
> *3° la communication non autorisée par la loi d'un renseignement personnel;*
> *4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.*

Commentaires :

Cette définition est large et ne prend pas en compte de manière explicite la notion de violation de sécurité qui est présente dans d'autres lois comme le RGPD ou encore le code civil californien.

Le RGPD dispose par exemple que constitue une : « *violation de données à caractère personnel », une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* »[22].

Le Code Civil Californien retient une définition similaire : "*(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system*"[23].

[19] RGPD, art. 33.
[20] RGPD, art. 34.
[21] RGPD, art. 33.
[22] Art. 4 12).
[23] Cal. Civ. Code, par. 1798.82

Il est ainsi proposé d'amender la définition de la manière suivante : *«3.6. Pour l'application de la présente loi, on entend par «incident de confidentialité» toute violation des mesures de sécurité entraînant:*

1° l'accès non autorisé par la loi à un renseignement personnel;
2° l'utilisation non autorisée par la loi d'un renseignement personnel;
3° la communication non autorisée par la loi d'un renseignement personnel;
4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

> ***Article 3.7.*** *Lorsqu'elle évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, la personne qui exploite une 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. Elle doit également consulter son responsable de la protection des renseignements personnels.*

Commentaires*:*

Il est appréciable que le projet de loi présente un référentiel au regard duquel le risque de préjudice doit être apprécié. Cet article ne met cependant pas assez l'accent sur les risques pour les droits et libertés de la personne dont les renseignements personnels sont concernés par l'incident de confidentialité. Cette notion de risque pour les droits et libertés de la personne concernée est une notion clé dans le RGPD en matière de violation de données à caractère personnel[24] et permet d'apprécier l'incident de confidentialité au regard du préjudice qu'il peut causer pour les personnes dont les renseignements personnels sont compromis, et non pas au regard du préjudice pour l'entreprise ou pour un tiers. Par ailleurs, une précision en ce sens permettrait de clarifier la notion de préjudice sérieux et les cas où celui-ci sera retenu, apportant ainsi une plus grande prévisibilité pour les entreprises.

> ***Article 3.8****. La personne qui exploite une entreprise doit tenir un registre des incidents de confidentialité. Un règlement du gouvernement peut déterminer la teneur de ce registre. Sur demande de la Commission, une copie de ce registre lui est transmise.*

Commentaires:

Dans une démarche de responsabilisation des entreprises, il apparaît normal que ces dernières tiennent un registre des incidents de confidentialité. Néanmoins, il nous semble que l'exacte teneur de ces registres doit être discutée avec les acteurs des différentes industries afin qu'elle soit en accord avec les différentes pratiques et problématiques propres à chaque secteur. Par ailleurs, il faut que le règlement du gouvernement visant à déterminer la teneur du registre tienne compte du fait que certaines informations sur un incident de confidentialité ne sont pas toujours connues de l'entreprise, comme les conséquences de l'incident par exemple. Par ailleurs, le règlement doit prévoir que s'il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être consignées dans le registre de manière échelonnée au fur et à mesure que l'entreprise en prend connaissance.

- Collecte des renseignements personnels

> ***Article 4.*** *Toute personne qui exploite une entreprise et qui, en raison d'un intérêt sérieux et légitime, recueille des renseignements personnels sur autrui doit, avant la collecte, déterminer les fins de celle-ci.*

[24] RGPD, art. 33

Commentaires :

La nouvelle rédaction de cet article correspond au principe de limitation des finalités, présent également dans le RGPD.[25]

En revanche, la notion d'intérêt sérieux et légitime mériterait d'être clarifiée, tant dans sa définition que dans son champ d'application. En effet, il semble que la loi actuelle, ainsi que le projet de loi, prévoient deux fondements qu'une entreprise peut utiliser pour collecter des renseignements personnels: le consentement de la personne concernée et l'exécution d'un contrat commercial. Or, la loi semble ici conditionner la collecte des données à un intérêt sérieux et légitime. S'agit-il donc d'une alternative pour les entreprises, leur permettant de collecter des renseignements personnels sur ce fondement, ou bien d'une exigence supplémentaire que l'entreprise doit remplir, en plus de justifier du consentement de la personne concernée ou de l'exécution d'un contrat commercial? Dans les deux cas, au vu de l'importance cruciale de cette notion et des conséquences sur la responsabilité de l'entreprise, une définition s'impose.

- Politique de confidentialité

> ***Article 8.2.*** *La personne qui recueille par un moyen technologique des renseignements personnels doit publier sur le site Internet de l'entreprise, le cas échéant, et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. Elle fait de même pour l'avis dont toute modification à cette politique doit faire l'objet.*

Commentaires:

Contrairement à l'article 3.2 du projet de loi, cet article fait ici clairement référence à des politiques de confidentialité externes qui doivent être mises à disposition des personnes concernées afin de remplir l'obligation d'information sur le traitement qui est fait de leur renseignement personnel. En ce sens, et comme nous l'avons souligné plus haut, il est normal que ces politiques soient publiques et accessibles à tous. La présence de cet article renforce néanmoins notre impression que, par opposition, l'article 3.2 fait référence uniquement aux politiques internes de l'entreprise. Nous réitérons donc notre souhait que ces dernières soient uniquement disponibles au sein de l'entreprise ou, le cas échéant, aux autorités, mais qu'elles ne soient pas communiquées publiquement.

- La notion de consentement manifeste, libre, éclairé et donné à des fins spécifiques

> ***Article 8.3.*** *Toute personne qui fournit ses renseignements personnels suivant l'article 8 consent à leur utilisation aux fins visées au paragraphe 1° du premier alinéa de cet article.*

Commentaires:

Nous suggérons de clarifier que le consentement implicite énoncé à l'art. 8.3 de la LPRPSP (art. 99 de la Loi 64) constitue un consentement manifeste, libre, éclairé et donné à des fins spécifiques au sens de l'article 14 alinéa 1 de la LPRPSP (art. 102 du PL 64) , dans le cas de renseignement personnel non sensible. En effet, un consentement implicite devrait être suffisant lorsque des renseignements personnels non sensibles sont collectés pour les fins divulguées à la politique de confidentialité de l'entreprise concernée.

[25] Article 5 du RGPD

- Protection par défaut

> ***Article 9.1.*** *Une personne qui exploite une entreprise et qui recueille des renseignements personnels en offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou de ce service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée*

Commentaires :

Nous saluons cette disposition dans la mesure où elle insère la notion de protection des données par défaut. En revanche, le langage utilisé devrait selon nous être précisé car, interprété *stricto sensu*, il impose des obligations disproportionnées aux entreprises. Il apparaît ainsi essentiel d'amender le langage afin de subordonner la mise en place de mesures de confidentialité au contexte entourant le traitement du renseignement personnel. L'article 25 du RGPD, relatif à la protection des données dès la conception et par défaut, est très éloquent à cet égard:

"*Compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en oeuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriée (...)".*

Cette formulation permet de donner davantage de flexibilité aux entreprises qui pourront adapter leurs "mesures techniques et organisationnelles" au risque global présenté par le traitement du renseignement ainsi qu'au coût de mise en œuvre.

Amendement proposé:

« 9.1 Une personne qui exploite une entreprise et qui recueille des renseignements personnels en offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou de ce service assurent ~~le plus haut niveau~~ un niveau adéquat de confidentialité compte-tenu de l'état de la technique, des coûts de mise en œuvre, du contexte et de la finalité du traitement ainsi que des risques pour les personnes concernées , sans aucune intervention de la personne concernée »

III. Caractère confidentiel des renseignements personnels

- Renseignement sensible

> ***Article 12.*** *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.*
>
> *Un renseignement personnel peut toutefois être utilisé à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants:*
> *1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;*
> *2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;*
> *3° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.*
>
> *Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli. Toutefois, ne peut être considérée comme une fin compatible la prospection commerciale ou philanthropique.*
>
> *Pour l'application de la présente loi, un renseignement personnel est :*
> *1° dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée;*
> *2° sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.*

Commentaires :

Alinéa 1: la lecture *a contrario* de cet article de cet alinéa :

- renforce l'idée selon laquelle il pourrait y avoir un nouveau type de base légale pour traiter une renseignement personnel (relevée à l'article 4) qui serait distinct du consentement. Est-ce qu'il est ici fait référence à l'intérêt sérieux et légitime? Il est en tout état de cause fondamental que la LPRPSP précise clairement toutes les bases juridiques sur lesquelles une entreprise peut se fonder pour traiter un renseignement personnel.
- laisse penser que le consentement peut être implicite en cas de collecte ou de communication à un tiers de renseignements considérés comme non sensibles. Ce faisant, le projet de loi s'aligne sur la loi fédérale, i.e. la Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDE ») et ses Lignes directrices pour l'obtention d'un consentement valable[26], qui prévoient explicitement la possibilité d'avoir un consentement implicite dans certaines situations.

Par ailleurs, cet alinéa introduit trois nouvelles exceptions au consentement. L'exception posée au 1° n'appelle pas d'observations particulières dans la mesure ou les fins considérées comme compatibles sont détaillées dans l'alinéa 3, avec l'exception notable de la prospection commerciale ou philanthropique qui ne peut être considérée comme compatible. La deuxième exception en revanche apparaît comme trop vague et sujette à interprétation car il est difficile d'affirmer avec certitude ce qui peut être une utilisation au bénéfice de la personne concernée. Afin d'éviter des incertitudes et une imprévisibilité, tant pour entreprises que pour les personnes concernées, il convient d'apporter des clarifications et des lignes directrices sur ce qui peut être considéré comme une utilisation au bénéfice de la personne concernée.

De plus, le projet de loi ne prend pas en compte le consentement en matière d'emploi, qui apparaît inadapté aux relations employeur-employé[27]. En effet, au vu de la dépendance résultant de la relation employeur/employé, il est peu probable que la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives suite à ce refus. Le consentement peut donc difficilement être donné librement, condition du consentement pourtant déjà prévue dans la LPRPSP et réitérée à l'article 14 du projet de loi. L'exemption au consentement en matière d'emploi est d'ailleurs prévue dans les autres lois provinciales, en Colombie-Britannique[28] et en Alberta[29].

Alinéa 4: La définition de la notion de renseignement sensible est saluée mais devrait être ici précisée dans la mesure où le critère de « haute attente raisonnable en matière de vie privée » est un critère subjectif et non objectif ce qui laisse place à l'interprétation. Étant donné qu'il existe une obligation de consentement exprès en présence de données sensibles prévue au premier alinéa de ce même article, il apparaît donc nécessaire de délimiter précisément ce que l'on entend par « renseignement sensible » à l'instar de l'article 9 du RGPD par exemple.

- Communication de renseignements personnels à l'extérieur du Québec

> ***Article 17***. *Avant de communiquer à l'extérieur du Québec un renseignement personnel, la personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée. Elle doit notamment tenir compte des éléments suivants:*
> *1° la sensibilité du renseignement;*
> *2° la finalité de son utilisation;*
> *3° les mesures de protection dont le renseignement bénéficierait;*
> *4° le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment son degré d'équivalence par rapport aux principes de protection des renseignements personnels applicables au Québec.*

[26] Commissariat à la protection de la vie privée du Canada, Lignes directrices pour l'obtention d'un consentement valable, Mai 2018
[27] Voir en ce sens le Groupe de travail de l'article 29 et ses lignes directrices sur le consentement au sens du règlement 2016/679, WP259 rév.01
[28] British Columbia - Personal Information Protection Act, Article 13: "(1) Subject to subsection (2), an organization may collect employee personal information without the consent of the individual."
[29] Alberta - Personal Information Protection Act, Article 15: "(1) An organization may collect personal employee information about an individual without the consent of the individual if (...)

La communication peut s'effectuer si l'évaluation démontre que le renseignement bénéficierait d'une protection équivalant à celle prévue à la présente loi. Elle doit faire l'objet d'une entente écrite qui tient 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.

Il en est de même 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.

Le présent article ne s'applique pas à une communication prévue au paragraphe 7° du premier alinéa de l'article 18.

Article 17.1. *Le ministre publie à la Gazette officielle du Québec une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec.*

Commentaires:

Alinéa 1: Le principe d'une évaluation des facteurs relatifs à la vie privée avant de communiquer des renseignements personnels hors du Québec nous apparaît tout à fait louable. En revanche, il nous semble impératif que la loi soit plus précise sur le type d'évaluation demandée et le degré de formalité requis. La profondeur de l'analyse et sa formalité devraient être proportionnées au degré de risque du transfert et au type de renseignement personnel transféré par exemple. De plus, une entreprise qui effectue des transferts hors du Québec de façon régulière et dans plusieurs pays du monde ferait face à un processus contractuel très lourd puisqu'elle devrait mettre en place des contrats dans le cadre de chaque transfert. Par ailleurs, certaines entreprises au Québec utilisent déjà des Clauses Contractuelles types adoptées par la Commission Européenne[30] dans le cadre de flux de données avec l'Union Européenne. Faut-il donc rajouter une entente écrite telle que mentionnée à l'article 17, en plus des clauses contractuelles types, dans le cadre de chaque transfert ?

Par ailleurs, l'article mentionne que l'analyse devrait prendre en compte le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment son degré d'équivalence par rapport aux principes de protection des renseignements personnels applicables au Québec. Cette analyse nous semble très lourde et difficilement réalisable pour tous les pays du monde au cas par cas, notamment pour des entreprises aux effectifs et aux ressources de personnes en charges de la conformité de la vie privée réduites. Nous comprenons de l'article 17.1 qu'une liste d'États, dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec, sera publiée dans le futur. Aucune date n'a cependant été fixée à l'heure actuelle.

En l'état actuel des choses, les obligations imposées par l'article 17 nous paraissent donc disproportionnées et impossibles à mettre en place dans la plupart des entreprises et pourraient ralentir considérablement le moindre flux de données. Nous appelons donc à:

- l'allégement de l'évaluation devant être effectuée avant un transfert et notamment la suppression de la prise en compte du régime juridique applicable dans l'État où ce renseignement serait communiqué;
- la publication au plus vite de la liste d'États dont le régime juridique est jugé équivalent aux principes de protection des renseignements personnels applicables au Québec;
- Une clarification du régime applicable pour ce qui relève des transferts à l'intérieur du Canada.

[30] RGPD, art. 46

- Communication d'un renseignement personnel à un tiers

> ***Article 18.3.*** *Une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise qu'elle confie à cette personne ou à cet organisme.*
>
> *Dans ce cas, la personne qui exploite une entreprise doit :*
> *1° confier le mandat ou le contrat par écrit;*
> *2° indiquer, dans le mandat ou le contrat, les mesures que le mandataire ou l'exécutant du contrat doit prendre pour assurer la protection du caractère confidentiel du renseignement personnel communiqué, pour que ce renseignement ne soit utilisé que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne le conserve pas après son expiration. Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service ou d'entreprise visé au premier alinéa doit aviser sans délai le responsable de la protection des renseignements personnels 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 il doit également permettre au responsable de la protection des renseignements personnels d'effectuer toute vérification relative à cette confidentialité.*
> *Le paragraphe 2° du deuxième alinéa ne s'applique pas lorsque le mandataire ou l'exécutant du contrat est un organisme public au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ou un membre d'un ordre professionnel.*

Commentaires:

Cet article prévoit la possibilité pour les entreprises de communiquer un renseignement personnel à un mandataire ou à un prestataire de services, sans obtenir le consentement de la personne concernée, si cette communication est nécessaire à l'exercice du mandat ou à l'exécution du contrat de service. Il entérine donc une situation très courante dans la vie des entreprises.

Il prévoit également qu'un contrat écrit doit prévoir les mesures que le mandataire ou le prestataire de service doit prendre afin d'assurer la protection du caractère confidentiel du renseignement personnel communiqué. En cela, il s'agit d'un mécanisme similaire à ce qui se trouve dans l'article 28 du RGPD qui prévoit que le traitement par un sous-traitant de données personnelles est régi par un contrat ou à l'article 1798.140 (v) et (w) du CCPA. Néanmoins, à la différence du RGPD ou du CCPA, le PL 64 ne prévoit pas de répartition des responsabilités entre le responsable principal des renseignements personnels et celui auquel il sous-traite les données. Il n'y a donc aucune responsabilité prévue du prestataire en cas de manquement à ses obligations autre qu'un manquement contractuel. Par ailleurs, le PL 64 n'évoque pas donc plus la chaîne de responsabilités lorsqu'un sous-traitant sous-traite à son tour certaine activités de traitement impliquant des renseignements personnels.

Comme mentionné précédemment, il serait donc judicieux ici qu'il existe une distinction entre l'entreprise qui contrôle les finalités et les moyens du traitement (la personne en charge) et la personne qui traite les renseignements pour le compte de la personne en charge. Une telle distinction permettrait ainsi de bien délimiter les rôles et responsabilités de chacun des acteurs qui sont impliqués dans un traitement de données.

- Anonymisation

> ***Article 23.*** *Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser, sous réserve d'un délai de conservation prévu par une loi.*
>
> *Pour 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.*
>
> *Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues.*

Commentaires:

Alinéa 2: La notion d'anonymisation est très importante et mériterait d'être plus développée, en détaillant notamment les mesures qui sont mises en place pour s'assurer que le renseignement a bien été anonymisé et non simplement pseudonymisé. Dans le cas d'une pseudonymisation, la ré-identification de la personne concernée est possible, par le recours par exemple à des informations supplémentaires. A cet égard, les mesures détaillées dans le CCPA pour empêcher une telle réidentification sont particulièrement pertinentes: *"Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:*

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
(2) Has implemented business processes that specifically prohibit reidentification of the information.
(3) Has implemented business processes to prevent inadvertent release of deidentified information.
(4) Makes no attempt to reidentify the information[31].

Les lignes directrices du groupe de travail de l'article 29[32] mettent en avant des critères similaires et liste trois questions qu'une entreprise pour déterminer si une donnée est réellement anonymisée:

- est-il toujours possible d'isoler un individu?
- est-il toujours possible de relier entre eux les enregistrements relatifs à un individu? et
- peut-on déduire des informations concernant un individu?

Le projet de loi pourrait s'inspirer de ces modèles afin de clarifier ce qu'est un renseignement personnel anonymisé ainsi que les techniques qui peuvent être mises en place par une entreprise pour s'assurer qu'il s'agit bien d'une anonymisation et non d'une simple pseudonymisation.

IV. Droits des personnes concernées

> ***Article 27****. Toute personne qui exploite une entreprise et détient un renseignement personnel sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication de ce renseignement en lui permettant d'en obtenir une copie.*
>
> *À la demande du requérant, un renseignement personnel informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible. À moins que cela ne soulève des difficultés pratiques sérieuses, un renseignement personnel informatisé recueilli auprès du requérant lui est, à sa demande, communiqué dans un format technologique structuré et couramment utilisé. Ce renseignement est aussi communiqué à sa demande à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement.*

[31] CCPA, Article 1798.140 (h)
[32] Lignes directrices du G29 sur les techniques d'anonymisation, WP216

Lorsque le requérant est une personne handicapée, des mesures d'accommodement raisonnables doivent être prises, sur demande, pour lui permettre d'exercer le droit d'accès prévu par la présente section.

Commentaires:

Cette section vient faire écho au droit d'accès à un renseignement personnel qui existe déjà dans la LPRPSP. Néanmoins, elle vient ajouter une obligation de fournir une copie dans un format structuré et couramment utilisé, ce qui rappelle en ce sens le droit à la portabilité des données prévu par le CCPA dans le cadre du droit d'accès et, dans des conditions limitées, par le RGPD. L'introduction d'un tel droit doit être saluée. En revanche, il nous apparaît important de prendre en compte la capacité de l'entreprise à pouvoir fournir ce renseignement personnel dans un format technologique structuré et couramment utilisé. Celle-ci doit déployer des efforts raisonnables en ce sens mais ne peut offrir aucune garantie.

Amendement proposé:

Article 27. *Toute personne qui exploite une entreprise et détient un renseignement personnel sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication de ce renseignement en lui permettant d'en obtenir une copie.*

À la demande du requérant, un renseignement personnel informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible. À ~~moins que cela ne soulève des difficultés pratiques sérieuses~~, L'entreprise déploie des efforts raisonnables pour communiquer au requérant un renseignement personnel informatisé ~~recueilli auprès du requérant lui est, à sa demande, communiqué~~ dans un format technologique structuré et couramment utilisé. Ce renseignement est aussi communiqué à sa demande à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement
Lorsque le requérant est une personne handicapée, des mesures d'accommodement raisonnables doivent être prises, sur demande, pour lui permettre d'exercer le droit d'accès prévu par la présente section.

- Obligation de prêter assistance au requérant dans le cas d'une demande de l'exercice de ses droits

Article 34. *Le responsable de la protection des renseignements personnels doit motiver tout refus d'acquiescer à une demande et indiquer la disposition de la loi sur laquelle ce refus s'appuie, les recours qui s'offrent au requérant en vertu de la présente loi et le délai dans lequel ils peuvent être exercés. Il doit également prêter assistance au requérant qui le demande pour l'aider à comprendre le refus.*

Commentaires:

Il nous semble que le simple fait que le responsable de la protection des renseignements personnels ait à motiver son refus représente une garantie suffisante que ce refus sera basé sur des motifs suffisamment sérieux et aisément vérifiables. En ce sens, l'obligation qui est faite au responsable de prêter assistance au requérant qui le demande de l'aider à comprendre le refus nous apparaît trop exigeante et dépourvue de valeur ajoutée puisque les motifs du refus seront déjà explicités clairement dans la réponse qui est faite au requérant. Nous proposons donc de supprimer cette dernière phrase.

Amendement proposé:

Article 34: *Le responsable de la protection des renseignements personnels doit motiver tout refus d'acquiescer à une demande et indiquer la disposition de la loi sur laquelle ce refus s'appuie, les recours qui s'offrent au requérant en vertu de la présente loi et le délai dans lequel ils peuvent être exercés. ~~Il doit également prêter assistance au requérant qui le demande pour l'aider à comprendre le refus.~~*