CI– 012M
C.P. – PL 64
Protection des
renseignements
personnels

# Moderniser, mais conserver un équilibre

Mémoire présenté à la

**Commission des institutions de l’Assemblée nationale du Québec**

dans le cadre des

**Consultations particulières et auditions publiques sur le Projet de loi n° 64 : *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels***

par

**M<sup>es</sup> Antoine Aylwin, Karl Delwaide, Jennifer Stoddart, Julie Uzan-Naulin, Guillaume Pelegrin, Aya Barbach et William Deneault-Rouillard**

MONTRÉAL, 23 SEPTEMBRE 2020

# Table des matières

# Présentation des auteurs

Les auteurs sont tous avocats membres du Barreau du Québec (ainsi que du Barreau de Paris pour certains) et exercent leur profession au sein du groupe de pratique national *Protection de l'information et de la vie privée* du cabinet *Fasken*.

Avocats issus de la pratique privée exerçant dans un cabinet canadien avec une présence internationale, ils ont l'opportunité de côtoyer sur une base quotidienne des entreprises diverses, allant de la start-up à la très grande entreprise, ainsi que des organismes publics et parapublics. Ils possèdent une vaste expérience dans les domaines de la protection des renseignements personnels et de l'accès aux documents des organismes publics, que ce soit en vertu des lois du Québec ou celles relevant du fédéral en semblables matières. Ils conseillent notamment leurs clients sur l'interprétation et l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (« **Loi sur l'accès** »), la *Loi sur la protection des renseignements personnels dans le secteur privé* (« **Loi sur le secteur privé** »), la *Loi* (fédérale) *sur l'accès à l'information*, la *Loi* (fédérale) *sur la protection des renseignements personnels*, la *Loi* (fédérale) *sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDÉ** ») et la *Loi concernant le cadre juridique des technologies de l'information* et le *Règlement général* (européen) *sur la protection des données* (« **RGPD** »).

Ils représentent leurs clients devant les divers tribunaux et organismes qui ont pour mission de décider des différends dans ces domaines, que ce soit la Commission d'accès à l'information du Québec, la Cour du Québec, le Commissariat à la protection de la vie privée du Canada et la Cour fédérale.

Chacun des auteurs publie régulièrement des articles et donne des conférences en matière de protection des renseignements personnels et d'accès à l'information. Le cabinet *Fasken* a d'ailleurs été élu cabinet juridique de l'année en droit de la protection de la vie privée et de la sécurité des données dans l'édition 2021 du guide *Best Lawyers in Canada*[1].

Le présent mémoire n'est pas le fruit d'une réflexion isolée. Il s'inscrit dans la droite ligne d'une série de documents produits par les soussignés concernant la Loi sur l'accès et la Loi sur le secteur privé, notamment :

- Mémoire de M$^{es}$ Karl Delwaide, Antoine Aylwin, Myriam Robichaud et Marc-André Boucher sur les propositions de modifications de la Loi sur l'accès contenues au document intitulé « Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels », en date de mars 2015, présenté à la Commission des institutions de l'Assemblée nationale du Québec le 4 septembre 2015 ;

- Consultations de M$^{es}$ Karl Delwaide et Antoine Aylwin relatives à l'actualisation de la Loi sur le secteur privé, transmis à Me Jean Chartier, président de la Commission d'accès à l'information du Québec, le 25 novembre 2015 ;

---

[1] BEST LAWYERS, « Announcing the 15th Edition of The Best Lawyers in Canada », *Best Lawyers*, 26 août 2020, en ligne : < https://www.bestlawyers.com/article/best-lawyers-canada-2021/3104 >.

- Document de discussion sur le consentement de M$^{es}$ Karl Delwaide et Antoine Guilmain, « Consentement et protection de la vie privée : regarder le passé, préparer l'avenir », présenté au Commissariat à la protection de la vie privée du Canada, août 2016 ;

- Mémoire de M$^{es}$ Karl Delwaide, Antoine Aylwin et Antoine Guilmain, « Maintenir un équilibre » relatif au rapport quinquennal de 2016 la Commission d'accès à l'information du Québec présenté à la Commission des institutions de l'Assemblée nationale du Québec, 1$^{er}$ juin 2017 ;

- M$^{es}$ 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 ;

- Bulletins hebdomadaires portant sur les différentes propositions du Projet de loi[2].

Les auteurs s'appuient donc sur leur vaste expérience et leurs connaissances de pointe en protection des renseignements personnels pour formuler leurs commentaires à l'endroit du Projet de loi n° 64 à la Commission des institutions.

Plus particulièrement, Antoine Aylwin est cochef national du groupe de pratique *Protection de l'information et de la vie privée* du cabinet *Fasken*. Il a développé, au fil des ans, une pratique élaborée en matière de protection des renseignements personnels et d'accès à l'information. Ses connaissances approfondies des technologies de l'information lui permettent d'ailleurs d'être au fait des défis auxquels font face les entreprises et les organismes publics. Il est également coauteur avec Me Delwaide de l'ouvrage intitulé *Leçons tirées de dix ans d'expérience : La Loi sur la protection des renseignements personnels dans le secteur privé du Québec*, 2005 (révisé en 2007).

Karl Delwaide est un praticien reconnu dans les domaines de l'accès à l'information et de la protection des renseignements personnels, ayant développé ceux-ci depuis 1987. Grâce à sa vaste expérience et à ses nombreux succès en litiges complexes, il est reconnu comme l'un des rares plaideurs québécois à avoir acquis une solide connaissance de tous les tribunaux en matière de protection de l'information et de la vie privée. Il est l'un des auteurs mandatés par le Commissariat à la protection de la vie privée du Canada pour écrire l'ouvrage intitulé *Leçons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé du Québec*, 2005 (révisé en 2007).

---

[2] FASKEN, « Série spéciale - Projet de loi 64 et la réforme des lois québécoises sur la protection des renseignements personnels » dans Bulletin, *Fasken*, 22 juin 2020, en ligne : < https://www.fasken.com/ fr/knowledge/projet-de-loi-64/2020/06/accueil/ >.

# Introduction

C’est avec plaisir que nous intervenons dans le cadre des consultations particulières sur le Projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[3] (« **Projet de loi** »), présenté le 12 juin 2020.

Compte tenu de l’ampleur du Projet de loi, nous faisons le choix de nous concentrer sur certains amendements qui y sont proposés. Nous souhaitons ainsi apporter un éclairage utile sur certains des enjeux découlant des propositions de modifications aux lois québécoises relativement à la protection des renseignements personnels.

De prime à bord, tel que prôné dans notre Mémoire présenté à la Commission des institutions (la « **Commission** ») en 2016[4] nous persistons à croire que doit subsister dans toute législation en matière de protection des renseignements personnels et d’accès à l’information une forme d’équilibre[5]. D’abord, un équilibre entre le droit à la vie privée et d’autres intérêts légitimes qui se justifient dans le cadre d’une société libre et démocratique, comme la sécurité publique, les relations internationales, le commerce électronique, etc. Mais aussi, un équilibre entre les approches divergentes de part et d’autre du globe. La protection des renseignements personnels doit s’exercer dans un cadre réglementaire qui n’est pas trop onéreux pour les entreprises.

Ensuite, en cette période de crise sanitaire lors de laquelle la transformation numérique s’accélère, la province de Québec consolide depuis quelques années sa pole position économique et scientifique en matière d’intelligence artificielle et les initiatives de « ville intelligente ». Il est donc primordial de s’assurer que la refonte de notre législation ne soit pas un frein à l’investissement et à l’innovation technologiques. Tout au contraire, notre législation doit être un moteur de croissance, de compétitivité et d’attractivité pour la province de Québec, ses villes et ses habitants.

Nous considérons que l’analyse d’impact réglementaire du Projet de loi menée par le Conseil du trésor, relativement notamment à l’estimation d’un coût de 68 000 000 $ pour les entreprises québécoises[6], est largement sous-évaluée. À vrai dire, nous soumettons respectueusement à la Commission que l’adoption du Projet de loi dans sa mouture actuelle serait beaucoup trop onéreuse pour les entreprises en ce qui a trait à leur mise en conformité.

---

[3] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi n°64 (Présentation-12 juin 2020), 1re sess., 42e législ. (Qc) (ci-après « **Projet de loi** »).

[4] Karl DELWAIDE, Antoine AYLWIN et Antoine GUILMAIN, « Maintenir un équilibre », Mémoire présenté à la Commission des institutions de l’Assemblée nationale du Québec, Québec, 2017.

[5] *Id*., p. 4.

[6] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Loi visant principalement à instituer le Centre d’acquisitions gouvernementales et Infrastructures technologiques Québec*, Analyse d’impact réglementaire (préliminaire), Québec, en ligne : < https://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/loi_reglements_politiques/Analyse_impact_reglmentaire.pdf >.

## 1. Communication à l'extérieur du Québec (articles 27 et 103 du Projet de loi)

20 % du PIB québécois reposait sur les exportations vers les États-Unis en 2016. L'année suivante, 726 filiales d'entreprises américaines étaient établies au Québec[7] et la valeur des exportations de marchandises provenant du Québec à destination des États-Unis représentait 70,5 % du total des exportations québécoises de marchandises à l'international. Toujours en 2017, la valeur des exportations québécoises de marchandises vers ses voisins du sud représentait près de six fois (5,9 fois) celle des exportations québécoises de marchandises vers l'Union européenne (« **UE** »)[8]. En 2019, c'est 71,2 % des exportations québécoises qui sont allées aux États-Unis[9].

Au niveau fédéral, en négociant l'Accord Canada–États-Unis–Mexique, lequel est entré en vigueur le 1er juillet 2020, le Canada a consolidé le libre-échange avec ses partenaires nord-américains. Le gouvernement fédéral a également fait des efforts de diversification de ses partenaires économiques dans les dernières années, visibles notamment par la ratification de l'Accord économique et commercial global entre le Canada et l'UE entré en vigueur en quasi-totalité le 21 septembre 2017, lequel ouvre plus grand que jamais la porte vers ce marché de plus de 500 millions de consommateurs pour les exportateurs québécois[10].

Ces fortes relations commerciales ont toutefois un prix : une dépendance économique grandissante envers deux partenaires internationaux qui n'ont pas la même approche en matière de protection des données, laquelle limite l'autonomie québécoise en matière de politique étrangère.

### 1.1 (In)adéquation

C'est dans ce contexte que le Projet de loi propose qu'avant toute communication de renseignements personnels « à l'extérieur du Québec », les entreprises doivent procéder à une évaluation des facteurs relatifs à la vie privée (« **EFVP** »), en tenant compte, notamment, de la sensibilité du renseignement, de la finalité de son utilisation, des mesures de protection dont le renseignement bénéficierait et « *du 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* »[11]. Afin que le renseignement personnel soit légalement communiqué dans cet « État » hors Québec, l'évaluation devrait démontrer que le renseignement fera l'objet d'une protection équivalente à la Loi sur le secteur privé[12].

Faisant écho au quatrième facteur énoncé ci-dessus, le Projet de loi propose ainsi que le ministre analyse les juridictions étrangères et publie à la Gazette officielle du Québec « *une liste d'États dont le régime*

---

[7] Geneviève RENAUD, « Conjoncture – Bilan de l'année 2019 », (2020) 20-4 *Commerce international des marchandises du Québec*, Institut de la statistique du Québec, 1.

[8] *Id*.

[9] *Id*.

[10] CENTRE DE RÉFÉRENCE EN AGRICULTURE ET AGROALIMENTAIRE DU QUÉBEC, « Le marché européen s'ouvre à vous, soyez prêts ! », *CRAAQ*, 29 août 2017, en ligne : < https://www.craaq.qc.ca/Evenements-du-CRAAQ/le-marche-europeen-s_ouvre-a-vous-soyez-prets/e/2449 >.

[11] Projet de loi, art. 103

[12] *Id.*

*juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec* »[13].

En d'autres mots, les différentes avenues possibles suite à l'adoption du Projet de loi actuel seraient que a) le gouvernement ait déjà identifié un « État » comme offrant des garanties de protection équivalentes à celles du Québec, b) les entreprises aient à confier la lourde tâche à des conseillers juridiques de faire une analyse de droit comparé entre les régimes applicables dans une panoplie d'« États », tout en ayant à se munir d'une entente contraignante les liant avec leurs partenaires étrangers et qui leur imposeraient de respecter les mêmes règles qu'au Québec.

Les mécanismes de reconnaissance de régimes législatifs équivalents font progresser le droit à la vie privée en favorisant l'harmonisation des cadres applicables de part et d'autre du globe. Le RGPD, source d'inspiration de plusieurs propositions contenues dans le Projet de loi, permet le transfert de renseignements personnels à des tiers situés dans « le pays tiers, territoires ou secteurs déterminés dans ces pays tiers », comme le Canada, qui ont été désignés par les autorités européennes comme offrant un niveau de protection partiellement adéquat[14].

Nous assistons toutefois présentement à l'établissement de systèmes de bulles concurrentes à travers le monde. Alors que de plus en plus de pays adoptent cette approche en la modulant selon leurs propres critères, la Cour de Justice de l'Union européenne a, en juillet 2020, invalidé le *Privacy Shield*[15], accord international permettant de transférer des renseignements personnels à partir de l'UE vers des organisations situées aux États-Unis adhérant à ce mécanisme. Ceci crée des barrières au commerce international et, à long terme, donne naissance à des systèmes Internet parallèles et clos.

### 1.2 Expertise nécessaire et autres impacts du nouveau mécanisme

C'est donc dire que les organisations québécoises, prises dans cette impasse entre deux forces divergentes, devraient se fier notamment à l'évaluation du gouvernement du Québec quant aux garanties offertes par les multiples lois applicables outre-mer. Les ressources nécessaires pour analyser les juridictions extérieures afin de déterminer si elles disposent de protections adéquates de la vie privée seront considérables pour le Québec. L'UE dispose d'une vaste bureaucratie à forte capacité qui a passé des années à analyser l'équivalence de pays allant du Canada au Japon. Il est difficile de voir comment la fonction publique provinciale du Québec pourrait disposer des moyens administratifs nécessaires à une telle tâche.

Si le gouvernement n'établit pas rapidement une liste de juridictions présumées sûres ou que cette liste n'inclut pas les États-Unis (ou du moins les états américains importants), nous sommes d'avis que l'économie québécoise en sera sévèrement affectée. À vrai dire, le fardeau d'analyser les juridictions étrangères risque d'être très lourd pour les entreprises.

---

[13] *Id.*

[14] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (*Règlement général sur la protection des données*), art. 44 et 45 (ci-après « **RGPD** »).

[15] CJUE, 16 juillet 2020, aff. C-311/18, Data Protection Commissioner/Maximillian Schrems et Facebook Ireland.

Ce n’est pas que la vigueur économique du Québec qui soufrerait de cette nouvelle procédure. À titre d’exemple, dans le cadre d’études cliniques, les données provenant de sites médicaux exigent des flux transfrontaliers de renseignements personnels provenant du Québec avec une multitude de juridictions étrangères pour assurer la validité de l’étude et l’approbation de la mise en marché de médicaments. L’introduction d’une obligation préalable d’effectuer une EFVP serait grandement néfaste en ce qui a trait à l’efficacité des processus déjà en place à cette fin et pourrait retarder, voir même empêcher, la tenue de telles études en sol québécois, ce qui entraînerait la perte d’opportunité de traitements pour les patients du Québec. De plus, alors que certains traitements personnalisés de type thérapies génétiques sont fabriqués à l’extérieur du Québec, des patients québécois pourraient être privées de ces traitements innovateurs (notamment en oncologie ou maladies dégénératives) car ceux-ci impliquent un transfert de renseignements personnels (par exemple, des cellules) qui ne pourrait plus se faire vers des juridictions considérées comme moins protectrices.

Ainsi, nous soumettons que certaines alternatives devraient ainsi être proposées dans le Projet de loi, telles que des clauses contractuelles types qui sont plus adaptées au commerce digital international. En vertu du RGPD, les parties peuvent souscrire à des clauses contractuelles types ou adopter des règles d’entreprise contraignantes afin de préserver le même niveau de protection, quel que soit l’endroit où les renseignements personnels peuvent être transmis[16].

### 1.3 Notion d’« État »

Nous portons à l’attention du lecteur que la procédure prescrite à l’article 103 du Projet de loi permet qu’un renseignement personnel soit légalement communiqué dans un « État » hors du Québec. Cette formulation est boiteuse, la définition d’« État » étant variable et alimentant les débats politiques, philosophiques et sociologiques. La notion d’« État » n’est pas non plus clairement définie dans la jurisprudence pertinente ni dans les lois d’interprétation applicables. Ainsi, on peut se demander si une province ou un état doivent être évalués distinctement dans un pays où, comme le Canada ou les États-Unis, la législation est différente dans certaines portions du pays.

À titre de comparaison, le régime européen en matière d’adéquation pour le transfert transfrontalier fonctionne par « pays, territoire, ou secteurs déterminés » aux termes du RGPD :

> *44. Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assurent un niveau de protection adéquat.*

Nous vous soumettons par les présentes nos inquiétudes quant à la possibilité qu’une entreprise québécoise doive se soumettre à l’exercice prescrit à l’article 103 du Projet de loi afin de transférer des renseignements personnels vers une filiale située dans la province de l’Ontario, « à l’extérieur du Québec »[17] et laquelle province pourrait également être qualifiée d’« État » au sens du Projet de loi. À cet égard, il faut noter que les échanges commerciaux avec l’Ontario représentent plus de 60 % du commerce

---

[16] RGPD, art. 46.

[17] Projet de loi, art. 103.

interprovincial du Québec, alors que la zone économique Québec-Ontario est la quatrième en importance en Amérique du Nord, suivant celles de la Californie, du Texas et de New York[18].

Il serait donc opportun de clarifier le libellé de l'article 103 en ce qui a trait à la notion d'« État » et de référer à d'autres types de territoires et secteurs. Ainsi, la liste que le ministre devra publier dans la Gazette officielle du Québec pourrait inclure spécifiquement certains territoires régis par des règles distinctes par rapport aux autres territoires organisés au sein d'un même pays, tels des états américains particulièrement favorables à l'économie québécoise.

**Recommandations :**

1. Introduire le principe d'imputabilité du responsable du traitement de renseignements personnels sans égard à l'emplacement des données et sans obligation pour une analyse de droit comparé[19].

2. Introduire des alternatives à la détermination de l'adéquation des juridictions étrangères, telles que des clauses contractuelles types ou des règles d'entreprise contraignantes, plus adaptées au commerce digital international.

3. Clarifier la notion d'« État ».

## 2. Conséquences du non-respect des lois (articles 150 à 152 du Projet de loi)

Le Projet de loi introduit deux changements majeurs dans la façon dont les droits protégés par la Loi sur le secteur privé seraient susceptibles de sanction. D'une part, il remanie les outils à la disposition de l'appareil gouvernemental en introduisant un nouveau régime de sanctions administratives pécuniaires[20] tout en facilitant l'accès aux sanctions pénales[21]. D'autre part, le Projet de loi introduit une nouvelle cause d'action civile en cas d'atteinte à un droit conféré par la Loi sur le secteur privé ou par le *Code civil du Québec* et prévoit l'octroi de dommages-intérêts punitifs d'au moins 1 000 $ en cas d'atteinte intentionnelle ou résultant d'une faute lourde.

### 2.1 Introduction d'un régime de sanctions administratives pécuniaires

Le Projet de loi introduit un régime de sanctions « administratives » pécuniaires permettant l'imposition de sanctions en cas de contravention aux dispositions de la loi. Ces sanctions peuvent aller jusqu'à un maximum de 10 000 000 $ par contravention (ou 2 % du chiffre d'affaires). Malgré les sommes

---

[18] MINISTÈRE DE L'ÉCONOMIE ET DE L'INNOVATION, « Accord de commerce et de coopération Québec-Ontario (ACCQO) », *Ministère de l'économie et de l'innovation*, dans Accords commerciaux, Québec, en ligne : < https://www.economie.gouv.qc.ca/bibliotheques/accords-commerciaux/accords-commerciaux/accord-de-commerce-et-de-cooperation-quebec-ontario/ >.

[19] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel », Éditions OCDE, Paris, 2002, en ligne : < https://www.oecd-ilibrary.org/fr/science-and-technology/lignes-directrices-de-l-ocde-sur-la-protection-de-la-vie-privee-et-les-flux-transfrontieres-de-donnees-de-caractere-personnel_9789264296398-fr >.

[20] Projet de loi, art. 150.

[21] *Id*., art. 151.

importantes qui pourraient être réclamées aux administrés, ces derniers ne disposeraient pas des protections constitutionnelles associées au système pénal, dont le fardeau de preuve de l'absence de doute raisonnable, la protection contre les saisies sans mandat judiciaire ou encore la protection contre l'auto-incrimination. Ces sanctions seraient applicables à pratiquement tout manquement à la loi, puisqu'ils visent la personne qui « recueille, communique, utilise ou détruit des renseignements personnels en contravention avec les dispositions de la présente loi »[22].

Nous sommes d'avis que la façon dont le Projet de loi est structuré aura pour effet de décourager l'utilisation du régime pénal par l'Administration, comme par le passé, et tendre vers la création d'un régime pénal parallèle dit « administratif » qui suscitera de nombreuses contestations judiciaires.

En effet, le fait que le montant des sanctions administratives soit d'une telle ampleur aura pour effet de décourager l'administration d'avoir recours au système pénal en raison de la facilité relative d'imposition d'une sanction administrative par rapport à un véritable système pénal. En effet, pourquoi investir des ressources importantes requérant le support d'enquêteurs et de poursuivants pénaux pour obtenir une condamnation maximale de 25 000 000 $, alors qu'une sanction administrative d'un montant de 10 000 000 $ peut être imposée sur simple décision administrative.

Considérant les sommes importantes qui sont en jeu, il est à prévoir d'innombrables contestations lors desquelles sera remise en question la véritable intention de l'Administration dans l'imposition de la sanction, car si la motivation de l'administration était d'imposer une peine plutôt que d'encourager un retour à la conformité, alors la sanction aurait été imposée d'une façon illégale puisque privant l'administré des protections conférées par les Chartes des droits et libertés.

Par ailleurs, nous souhaitons sensibiliser les parlementaires aux ressources importantes qui seraient requises au sein de la Commission d'accès à l'information (« **CAI** ») pour la gestion de la délivrance et de la contestation des sanctions administratives pécuniaires. En effet, le Projet de loi prévoit, à son article 90.6, que ce serait un membre de la section surveillance de la CAI qui serait chargé d'entendre une contestation d'une sanction administrative pécuniaire.

Considérant les délais existants pour obtenir une audition pour des affaires simples, il nous apparait impossible de concevoir d'ajouter de nouvelles fonctions sans augmenter significativement les ressources disponibles. De plus, ces ressources additionnelles devraient aller au-delà de l'ajout de commissaires additionnels puisque la décision d'imposer une sanction administrative par la fonction administrative devrait être défendue par les avocats de la CAI devant la fonction juridictionnelle. Ainsi, c'est une toute nouvelle équipe d'avocats, de technologues et d'autres spécialistes dans l'évaluation de la mauvaise utilisation des renseignements personnels via des technologies en évolution constante, ayant un rôle comparable à celui de la police, qu'il faudrait ajouter aux effectifs de la CAI.

**Recommandations** :

---

[22] *Id*., art. 150.

4. Restreindre les sanctions administratives à des contraventions pour des transgressions de nature plus technique et ayant moins d'impact sur la vie privée, afin d'éviter la création d'un système parallèle qui brouille les frontières entre régimes administratif et pénal.

5. Augmenter significativement l'écart entre les montants maximums pouvant être réclamés pénalement et civilement selon un ratio pouvant être de 1 pour 20, soit dans l'hypothèse d'une amende maximale de 25 000 000 $, d'une sanction maximale de 125 000 $, laquelle serait tout de même largement suffisante pour assurer un retour rapide à la conformité dans un processus administratif.

### 2.2 Introduction d'une nouvelle cause d'action civile

Le nouvel article 93.1 de la Loi sur le secteur privé, proposé par le Projet de loi, introduit une nouvelle cause d'action en cas d'atteinte illicite à un droit conféré par la loi ou par les articles 35 à 40 du *Code civil du Québec*. Or, la rédaction de cet article pourrait lui donner une portée qui irait au-delà des objectifs de la loi puisque les articles 35 à 40 du *Code civil du Québec* ne traitent pas que de la protection des renseignements personnels, mais bien du respect de la réputation et de la vie privée. Ainsi, bien que ces concepts puissent se recouper, ce n'est pas toujours le cas. Par ailleurs, le fait de prévoir l'octroi de dommages-intérêts punitifs, ce qui est exceptionnel en droit québécois et, encore plus exceptionnel, un montant minimal prescrit, pose le risque de privatisation de la justice en plus de retirer aux juges leur pouvoir d'appréciation dans la fixation d'une sanction appropriée. En effet, cette nouvelle cause d'action risque d'encourager les actions collectives dans lesquelles une atteinte intentionnelle ou une faute lourde seront systématiquement alléguées afin de se qualifier pour l'octroi de dommages-intérêts punitifs.

**Recommandations** :

6. Étudier les conséquences d'inclure une référence aux articles 35 à 40 du *Code civil du Québec* dans le nouvel article 93.1 proposé dans la Loi sur le secteur privé.

7. Revoir l'opportunité de prévoir un montant minimal pour les dommages-intérêts punitifs afin de laisser la discrétion requise aux tribunaux dans l'octroi des dommages appropriés;

## 3. Exemption lors de « transaction commerciale » (article 107 du Projet de loi)

Il est proposé dans le Projet de loi d'introduire une exception spécifique au principe du consentement dans un contexte de « transaction commerciale ». Le nouvel article 18.4 qui serait ajouté à la Loi sur le secteur privé suite à l'adoption du Projet de loi permettrait la communication de tout renseignement personnel entre deux parties à une « transaction commerciale » envisagée, et ce sans avoir à obtenir le consentement des individus concernés, pour autant que la communication de ces renseignements personnels soit nécessaire aux fins de la conclusion de cette transaction et qu'une entente soit d'abord conclue entre les parties, prévoyant que la partie recevant communication des renseignements s'engage à établir des mesures de sécurité nécessaires et à restreindre son utilisation, sa rétention et sa communication ultérieure des renseignements personnels communiqués dans le cadre de cette « transaction commerciale »[23].

Il faut saluer cet amendement, attendu depuis longtemps ! Dans les faits, le Québec se met au diapason des autres lois canadiennes. Les lois fédérale[24], britanno-colombienne[25] et albertaine[26] en matière de protection des renseignements personnels prévoient déjà des exceptions très similaires au consentement dans le cadre de transactions commerciales.

Une observation s'impose toutefois quant à la définition qui serait donnée à la notion de « transaction commerciale » faisant l'objet de l'exception au consentement aux termes du Projet de loi, c'est-à-dire une transaction « *qui implique le transfert de propriété de tout ou partie de l'entreprise* ». Cette définition restrictive risque de diminuer l'efficacité de l'exception proposée, considérant que d'autres transactions telles que le financement par la dette, bien que nécessitant généralement elles aussi une vérification diligente préalable, n'impliquent pas à proprement parler de « transfert de propriété de tout ou partie de l'entreprise ».

Il serait donc pertinent de se pencher sur les définitions fournies par les autres lois canadiennes alors que celles-ci sont beaucoup plus larges. Par exemple, la loi fédérale définit les « transactions commerciales » de façon beaucoup plus détaillée, y incluant notamment « le fait de consentir un prêt à tout ou partie d'une organisation ou de lui fournir toute autre forme de financement »[27].

**Recommandation :**

8. Élargir la définition de « transaction commerciale » pour y inclure des concepts de financement par la dette, de prêt, de fusion et d'autres formes de réorganisation corporative n'impliquant pas nécessairement un « transfert de propriété de tout ou partie d'une entreprise ».

## 4. La place du consentement (articles 95 et 102 du Projet de loi)

À l'instar de ce que nous soumettions en 2016, nous estimons qu'un équilibre doive être trouvé entre la protection de la vie privée des individus et les besoins des entreprises de recueillir, utiliser ou communiquer des renseignements personnels dans le cadre de leurs activités commerciales légitimes. Pour ce faire, nous préconisions notamment que les entreprises informent convenablement les individus en prônant la « règle des 4 C » dans la rédaction des politiques de confidentialité, à savoir : cohérence, clarté, concision et caractère complet. Avant de nous pencher ci-après sur les commentaires propres aux dispositions telles que proposées dans le Projet de loi, nous soulignons d'emblée que deux principes importants sont absents du Projet de loi, lesquels mériteraient toutefois d'être mis en exergue : le principe de consentement implicite et l'exemption à la nécessité d'obtenir le consentement en contexte de relation d'emploi.

---

[23] Projet de loi, art. 107.

[24] Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5., art. 7.2 (ci-après LPRPDE).

[25] Personal Information Protection Act, SBC 2003, c. 63, art. 20 (ci-après « PIPA BC »).

[26] Personal Information Protection Act, SA 2003, c P-6.5, art. 22 (ci-après « PIPA A »).

[27] LPRPDE, art. 2(1).

### 4.1 L’obligation de devoir donner un consentement distinct de toute autre information communiquée

L’article 14 tel que proposé dans le Projet de loi dispose que le consentement doive être notamment demandé « distinctement » de toute autre information communiquée à la personne concernée pour chacune des fins visées. Cette obligation telle que présentement rédigée soulève toutefois des enjeux pratiques d’application, tant pour les entreprises que pour les individus.

Tant du point de vue des consommateurs que des entreprises, il semblerait contre-productif d’assaillir le consommateur d’autant de documents que d’objectifs poursuivis afin de tenter de s’enquérir d’un consentement valide. À notre sens, cette obligation irait à l’encontre de l’objectif poursuivi depuis des années afin de mettre en place des mécanismes d’information qui soient valides et efficaces pour le consommateur.

Il nous semble raisonnable d’avancer qu’un consentement puisse être demandé en des termes simples et clairs tout en énumérant de la même manière chaque finalité poursuivie dans un même formulaire de consentement. L’inverse risquerait d’avoir pour effet de « noyer » le consommateur avec un trop-plein d’information indigeste qui pourrait conduire à l’effet inverse que celui escompté. En effet, cette pratique risquerait d’avoir pour effet que le consommateur ne lise pas réellement l’information communiquée tout en ayant pour conséquence de conduire à un processus inefficace.

**Recommandation :**

9. Enlever l’obligation de devoir demander un consentement « distinct » pour chacune des fins visées, mais plutôt viser un principe de clarté.

### 4.2 Publication des politiques et pratiques encadrant la gouvernance des entreprises en matière de protection des renseignements personnels et commentaires au regard du principe de « proportionnalité » dans la rédaction de ces politiques

L’article 3.2, tel que proposé par le Projet de loi, dispose que les entreprises doivent établir et mettre en œuvre des politiques et des pratiques encadrant leur gouvernance à l’égard des renseignements personnels et propres à assurer la protection de ces renseignements personnels. Plus avant, l’article 3.2 proposé prévoit notamment que ces politiques soient 1) proportionnées à la nature et à l’importance des activités de l’entreprise et 2) que celles-ci soient publiées sur le site Internet de l’entreprise ou autrement rendu accessible par tout autre moyen.

Tout d’abord, il semblerait nécessaire d’obtenir des précisions quant à ce que constituerait une politique « proportionnée » eu égard à la nature et l’importance des activités de l’entreprise. En effet, si cela réfère au volume de la politique en tant que tel, nous estimons que ce n’est pas tant le nombre de pages que le contenu d’une politique et son intelligibilité par les membres de l’entreprise qui constituera une politique pertinente et efficace.

Par ailleurs, le fait d’exiger que ces politiques internes soient rendues publiques pourrait avoir l’effet inverse que celui escompté voire mettre en péril les mesures de sécurité prises par l’entreprise. En effet, nous estimons que le consommateur n’a pas besoin d’obtenir des informations propres aux mesures internes de l’entreprise pour être valablement informé sur le traitement fait de ses renseignements personnels. En effet, l'accent devrait davantage être mis sur l'importance de diffuser de l'information claire, concise, cohérente et complète (« Règle des 4 C ») afin d'informer valablement les individus plutôt que d'imposer aux entreprises de diffuser de l'information inutilement longue et potentiellement impertinente pour les individus par souci de satisfaire aux nouvelles obligations éventuelles comprises dans le Projet de loi.

En outre, il semble dangereux d'imposer aux entreprises de devoir rendre publiques les versions détaillées de leurs politiques et pratiques en matière de protection des renseignements personnels. En effet, les mesures prises par les entreprises en matière de sécurité de l'information et protection des renseignements personnels comprennent des renseignements sensibles et confidentiels. Autrement dit, le fait de devoir rendre publiques les mesures prises pour assurer la protection des renseignements personnels et, de manière plus large, la sécurité de l'information risquerait de miner l'efficacité des programmes de sécurité mis en place par les entreprises. Les atteintes pourraient être plus nombreuses, sophistiquées et concluantes puisque l'infrastructure d'une entreprise pour contrer celles-ci n'aurait plus de surprise pour les personnes mal intentionnées. Ces renseignements peuvent par ailleurs constituer des renseignements commerciaux privilégiés pour les entreprises. Dans ce contexte, il n'est pas négligeable de considérer que le fait de devoir légalement être tenu de rendre public ce type de renseignements pourrait d'ailleurs conduire certaines entreprises à décider de ne pas faire affaire au Québec.

**Recommandations :**

10. Réviser l'imposition de devoir mettre en place des politiques proportionnées à la nature et à l'importance des activités pour davantage mettre l'accent sur l'obligation de devoir mettre en place des politiques courtes, claires, concises et cohérentes.

11. Retirer l'obligation de devoir publier les politiques et pratiques internes d'une entreprise sur son site Internet ou par tout autre moyen approprié.

### 4.3 Le consentement implicite

Nous comprenons que la notion de consentement implicite est indirectement comprise au Projet de loi puisque la nécessité d'obtenir un consentement de façon expresse est nécessaire uniquement lorsqu'il s'agit d'un renseignement sensible. Dans ce contexte, une lecture à contrario permet de déduire qu'un consentement implicite peut être admis lorsque les renseignements en cause ne sont pas « sensibles ».

Bien que cette formulation et cette interprétation soient en soi une avancée et confirment la position prise par la Commission d'accès à l'information dans son rapport quinquennal de 2016 (qui reconnait que le consentement puisse être « explicite ou implicite »), nous estimons qu'il serait bénéfique qu'à l'instar des autres lois canadiennes, la Loi sur le secteur privé encadre ce principe. En effet, il serait pertinent que la Loi sur le secteur privé prévoie expressément que le consentement implicite soit admis et pose le cadre et la balise pour que les entreprises puissent s'en prévaloir.

**Recommandation :**

12. La Loi sur le secteur privé devrait expressément autoriser le consentement implicite et prévoir ses critères d'application.

### 4.4 L'exemption au consentement en matière d'emploi

Tel que l'a soumis une récente doctrine proposant plusieurs amendements à la Loi sur le secteur privé, nous soumettons que le modèle de consentement actuel semble inadapté aux relations employeur-employé. Dans ce contexte, voici les arguments que soumettent Mes Antoine Guilmain et Éloïse Gratton, position à laquelle les auteurs se joignent :

> « Soulignons d'emblée que le modèle du consentement apparaît inadapté aux relations employeur-employé. Tout d'abord, on peut difficilement considérer le consentement d'un employé vis-à-vis de son employeur comme étant « libre », car un employé pourrait croire, à tort ou à raison, que son emploi est en jeu en cas de refus. De plus, si un employé refuse que son employeur puisse collecter, utiliser ou communiquer ses renseignements personnels à des fins normales d'emploi, cela pourrait tout simplement empêcher l'employeur de maintenir ses activités et de remplir ses obligations légales. Un tel constat n'a rien de nouveau et a notamment été observé par la Cour fédérale du Canada.
>
> Aussi, en vertu de la LPRPDÉ, PIPA (BC) et PIPA (Alberta), les employeurs peuvent, sans le consentement des employés, collecter, utiliser et communiquer les renseignements personnels qui sont nécessaires pour établir, gérer ou mettre fin à la relation d'emploi. Les employeurs ont néanmoins l'obligation d'informer au préalable les employés que leurs renseignements personnels seront ou pourraient être recueillis, utilisés ou communiqués à ces fins. En pratique, cette obligation d'information se manifeste par une notification aux employés, sous forme d'avis, leur expliquant quels renseignements personnels seront collectés, comment ils seront utilisés et potentiellement communiqués dans le cadre de leur emploi. Cela dit, les dispositions de ces lois ne règlent pas entièrement la problématique, puisque certaines situations pourraient légitimement conduire l'employeur à devoir communiquer les renseignements personnels de leurs employés bien que ce ne soit pas directement relié à la gestion de leur emploi.
>
> Au sein de l'Union européenne, il est admis que le consentement ne peut pas être « librement » donné par des employés puisqu'il y a un déséquilibre de rapports de force avec les employeurs. Aussi, les employeurs ne devraient pas se fonder sur le consentement de leurs employés pour pouvoir traiter leurs données personnelles, mais plutôt sur un autre fondement légal prescrit par le RGPD. Ainsi, les employeurs peuvent traiter les données personnelles de leurs employés lorsque le traitement est nécessaire soit pour l'exécution du contrat de travail, soit pour respecter les obligations légales de l'employeur ou encore dans le cadre de ses « intérêts légitimes »107. Ce faisant, tout en reconnaissant le caractère illusoire du consentement dans un contexte d'emploi, le RGPD impose aux employeurs la responsabilité de vérifier si leurs activités de traitement correspondent à l'un des motifs énumérés par la loi – bien que cette évaluation puisse être remise en question par les employés. »

Dans ce contexte, il est très courant de constater qu'il est souvent impossible, voire fastidieux, de recueillir le consentement explicite dans le contexte des relations employeurs-employés alors que la collecte de renseignements personnels est d'une part légitime et par ailleurs nécessaire afin de gérer la relation d'emploi. La notion de consentement comme pierre angulaire à la construction des lois applicables en matière de protection des renseignements personnels repose sur une prémisse inexacte. Dans les faits, il s'agit plutôt d'une relation basée sur la transparence des pratiques de l'utilisateur des renseignements personnels.

Par souci de cohérence notamment, il nous semble important que la Loi sur le secteur privé prévoie les mêmes modalités, à l'instar des autres lois canadiennes, quant à la possibilité de se prévaloir d'un consentement implicite en matière de relation d'emploi. Le mécanisme de notification aux employés en amont de la collecte, tel que prévu dans les autres lois canadiennes, permettrait d'assurer aux employeurs de traiter les renseignements personnels des employés en toute transparence et assurer ainsi un mécanisme efficace tout en sauvegardant la protection des renseignements personnels des employés.

**Recommandation :**

> 13. La Loi sur le secteur privé devrait être modifiée afin de prévoir une exception au consentement en matière d'emploi, dans le même sens que les lois canadiennes sur la protection des renseignements personnels.

## 5. Santé et recherche (articles 90, 102 et 110 du Projet de loi)

Les organisations engagées dans le développement et la fabrication de traitements innovants pullulent au Québec. Dans le contexte de crise sanitaire conjugué au développement rapide des technologies liées aux soins de santé, il est primordial de saisir cette opportunité pour façonner une réforme de la protection des renseignements personnels permettant des utilisations responsables et bénéfiques des données pour la recherche en santé et l'amélioration des résultats de recherche médicale. Dans cette « nouvelle normalité », nous soumettons à la Commission qu'il est temps pour le Québec de saisir cette occasion de démontrer que les lois sur la protection des données peuvent équilibrer les droits à la vie privée, tout en permettant d'améliorer les soins de santé et les traitements innovants pour ses citoyens.

### 5.1 Mécanisme d'accès aux données à des fins de recherche, d'étude et de statistique

D'abord, nous saluons l'approche prise dans le cadre des propositions d'amendement contenues dans le Projet de loi en ce qui a trait à la communication et à l'utilisation des renseignements personnels à des fins d'étude, de recherche ou de statistique et qui visent à retirer l'autorisation préalable de la CAI, vu notamment les enjeux de ressources énumérés ci-haut[28]. En effet, malgré la complexité du mécanisme proposé, de tels amendements à la Loi sur le secteur privé, à la Loi sur l'accès et à la *Loi concernant le partage de certains renseignements de santé* permettraient d'augmenter considérablement l'efficacité du mécanisme d'accès aux données à des fins de recherche et d'étude[29]. Le retrait de la nécessité d'obtenir l'approbation de la CAI est une proposition bénéfique, alors que cette approbation est généralement

---

[28] Projet de loi, art. 90 et 110.

[29] *Id.*

accordée après un an ou plus d'attente (les fonds de recherche sont souvent octroyés sur un cycle de trois ans)[30].

Toutefois, alors que d'autres provinces comme l'Alberta, la Colombie-Britannique et l'Ontario ont déjà simplifié les demandes d'accès des chercheurs dans le but de faciliter le progrès scientifique, l'urgence est bien présente au Québec.

On peut toutefois se demander si le processus prévu par la Loi n'est pas inutilement complexe, alors qu'un équilibre entre efficacité et conformité par une reddition de compte sur l'utilisation des renseignements se doit d'être documentée.

**Recommandation :**

14. Raccourcir au minimum possible le délai transitoire d'un an, suite à l'adoption du Projet de loi, pour l'entrée en vigueur des dispositions facilitant l'accès aux renseignements personnels à des fins d'étude, de recherche ou de statistique.

15. Valider avec le milieu scientifique que le processus proposé n'est pas inutilement complexe.

### 5.2 Mécanisme d'exemption au consentement pour l'utilisation interne à des fins secondaires

Cet aspect est étroitement lié à la question du consentement, abordée dans la Section 4 du présent Mémoire. Le Projet de loi propose de dispenser les organisations d'avoir à obtenir le consentement des individus concernés pour utiliser ces données à des fins secondaires dans les cas où (1) elles sont compatibles avec la finalité initiale (les utilisations à des fins de prospection commerciale ne sont pas considérées comme des utilisations compatibles), (2) elles profitent clairement à la personne concernée ou (3) elles sont utilisées à des fins de recherche ou de statistiques lorsque les données sont dépersonnalisées[31].

Il n'est pas clair, aux termes du Projet de loi et à la lumière de l'exigence de consentement ci-dessus (à demander pour chaque finalité spécifique), comment l'utilisation secondaire des données sera gérée dans le contexte de la recherche médicale ou de la recherche clinique, sachant qu'en général, ce type de recherche implique le traitement d'une quantité considérable de renseignements personnels. Il est, selon nous, nécessaire de clarifier si un consentement donné peut être suffisamment spécifique tout en permettant l'utilisation secondaire des données et, dans l'affirmative, quel niveau de spécificité serait requis.

Le Groupe de travail sur la gouvernance des données de la Fédération européenne des associations et industries pharmaceutiques a proposé de faire référence au domaine thérapeutique dans lequel le médicament expérimental est testé - par opposition à une référence spécifique au seul protocole - pour

---

[30] CONSEIL DES ACADÉMIES CANADIENNES, « L'accès aux données sur la santé et aux données connexes au Canada », rapport du *Conseil des Académies*, Ottawa, 2015, p. 47, 51 et 82.

[31] Projet de loi, art. 102.

permettre une utilisation secondaire dans le même domaine thérapeutique[32]. Cela pourrait constituer une avancée majeure, en particulier pour les analyses des taux de survie à l'aide de « données de survie », dans le cadre desquelles l'obtention du consentement de l'individu concerné est souvent impossible pour cause de décès, en raison du laps de temps écoulé.

Toujours à titre illustratif, une étude clinique réalisée en lien avec le cancer du sein par une entreprise du secteur privé pourrait finalement permettre la découverte d'une potentielle avancée en lien avec le développement du cancer des ovaires. Dans un tel cas, l'utilisation secondaire des données nécessitant un nouveau consentement pourrait être impossible, encore une fois en raison du temps écoulé depuis le consentement initial, ou en raison des difficultés pour retracer les individus concernés.

**Recommandations :**

16. Ajuster et clarifier l'exigence de spécificité du consentement à obtenir.

17. Permettre une utilisation secondaire des renseignements personnels dans un même domaine, voire plusieurs domaines thérapeutique.

## 6. Évaluation des facteurs relatifs à la vie privée (article 103 du Projet de loi)

Dans les dernières décennies, l'analyse d'impact sur la vie privée a pris une place accrue dans le domaine de la protection des données. Inspirée de l'étude d'impact environnementale, elle fait maintenant partie intégrante des bonnes pratiques de planification pour les nouvelles utilisations de renseignements personnels. Comme l'émergence de nouvelles technologies s'accélère sans cesse et qu'ils peinent à suivre ce rythme, les gouvernements et les organismes de réglementation exigent de plus en plus souvent une telle analyse pour les nouvelles activités qui requièrent le traitement de renseignements personnels.

Au niveau de l'Union européenne, avec le RGPD, les analyses d'impact, appelées « analyses d'impact relatives à la protection des données » (« AIPD »), ne sont plus seulement une bonne pratique : elles constituent une obligation dans bien des cas. Elles sont obligatoires lorsque le traitement de données envisagé « est susceptible d'engendrer un risque pour les droits et libertés » des personnes concernées, notamment en cas d'utilisation de nouvelles technologies[33]. Par conséquent, la responsabilité du respect de la vie privée ne repose plus uniquement sur les épaules des institutions ou des citoyens : elle incombe désormais à toutes les organisations.

Cette même approche est préconisée au Québec dans le Projet de loi, par l'article 95 proposant les nouveaux articles 3.3 et 3.4 de la Loi sur le secteur privé.

### a) L'évaluation d'impact au sens du Projet de loi

Plus précisément, le Projet de loi propose essentiellement d'obliger les entreprises privées à procéder à une évaluation des facteurs relatifs à la vie privée (« **EFVP** ») dans les hypothèses suivantes :

---

[32] LEEM, « EFPIA : European Federation of Pharmaceutical Industries and Associations », 31 janvier 2018, en ligne : < https://www.leem.org/efpia >

[33] RGPD, art. 35 et consid. 89 à 95.

- pour « 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 »[34];

- avant de communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques[35];

- avant de communiquer un renseignement personnel à l'extérieur du Québec[36].

La première hypothèse nous semble suffisamment large pour couvrir presque toutes les situations, puisqu'un système d'information est mis en place à chaque fois que des renseignements sont organisés au sein d'une entreprise.

Toute entreprise devra désormais effectuer une EFVP pour « tout projet de système d'information ou de prestation électronique de services »[37]. Le projet de loi va plus loin que le RGPD dans lequel l'AIPD n'est obligatoire qu'en raison du risque pour les droits et libertés des individus, car il requiert une évaluation pour tout nouveau projet et non uniquement ceux qui semblent à haut risque. Nous soumettons à la Commission que ceci représente un fardeau important pour beaucoup d'entreprises au Québec.

Le Projet de loi prévoit également que la personne responsable de la protection des renseignements personnels au sein de l'entreprise doit être consultée aux fins de l'EFVP. Il décrit ce que cette personne peut proposer, à toute étape du projet[38] :

- la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels;

- des mesures de protection des renseignements personnels dans tout document relatif au projet;

- une description des responsabilités des participants au projet en matière de protection des renseignements personnels;

- la tenue d'activités de formation sur la protection des renseignements personnels pour les participants au projet.

### b) Les insuffisances du Projet de loi quant à l'EFVP

Si le Projet de loi précise qu'une telle évaluation doit tenir compte a) de la sensibilité du renseignement, b) de la finalité de son utilisation, c) des mesures de protection dont le renseignement bénéficierait et d) du régime juridique applicable dans l'État où ce renseignement serait communiqué, il n'énonce pas les

---

[34] Projet de loi, art. 95

[35] *Id*., art.110.

[36] *Id*., art. 103.

[37] *Id*., art. 95.

[38] *Id*.

critères qui permettraient de déterminer si une EFVP est adéquate. Il ne dit rien au sujet du rôle du risque dans l'évaluation à effectuer. Il n'évoque pas non plus la mise en œuvre de l'évaluation dans le projet ni les éventuelles conséquences d'une évaluation incomplète ou d'une absence d'évaluation.

Notons que la Commission d'accès à l'information (la « **Commission** ») a produit un document de travail expliquant la marche à suivre pour procéder à une EFVP[39]. Toutefois, ce guide est paru avant le dépôt du Projet de loi; conséquemment, il présente l'EFVP comme un outil optionnel et pourrait donc être entièrement révisé suite à l'adoption du Projet de loi. Le guide indique les étapes du déroulement d'une EFVP.

> 1. Préparation : Cette étape consiste à définir le projet, le contexte organisationnel et les obligations de l'organisation en matière de protection de la vie privée et des renseignements personnels (recenser les renseignements personnels visés par le projet, évaluer leur degré de sensibilité et établir les interactions entre l'organisation et les renseignements personnels visés).
>
> 2. Réalisation : D'après le guide, les facteurs considérés comme « relatifs à la vie privée » et qui sont à évaluer sont les suivants :
>
> - La conformité du projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient, comme la détermination des fins, le consentement, la limitation de la collecte, de l'utilisation, de la divulgation et de la conservation, les mesures de sécurité et l'exactitude des renseignements recueillis.
>
> - L'identification des risques d'atteinte à la vie privée engendrés par le projet, par exemple la conservation de renseignements dont l'utilité n'est plus démontrée, le vol, la collecte excessive, la divulgation non autorisée ou la création excessive ou injustifiée de renseignements.
>
> - L'évaluation de l'impact des risques en matière de vie privée engendrés par le projet, qui peut être réalisée au moyen d'un système de notation. Dans tous les cas, il est important que les risques soient quantifiés et gérés et qu'un degré de risque acceptable soit établi en amont.
>
> - La mise en place de stratégies pour éviter ces risques ou les réduire efficacement : il peut s'agir d'un système de gestion des documents qui applique automatiquement un calendrier de conservation, d'un examen des procédures d'attribution et de gestion des accès informatiques, de l'embauche d'une firme de sécurité informatique pour examiner les paramètres de sécurité du produit ou du service, de la révision des clauses de confidentialité des contrats, etc.

---

[39] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée », mis à jour le 5 mai 2020, en ligne : < https://www.cai.gouv.qc.ca/documents/Guide_EFVP_FR.pdf >.

3. Préparation du rapport : La dernière étape du processus vise à consolider les résultats de l'évaluation et à attester de vos réflexions et de vos actions en cas de vérification, d'inspection ou d'enquête de la part d'un organisme de réglementation.

Or, tous ces éléments devraient se trouver dans le Projet de loi afin d'éviter toute ambiguïté.

**Recommandations** :

18. Circonscrire les cas où une EFVP devrait être réalisée, sur le modèle du RGPD, en cas de risque pour les droits et libertés des individus.

19. Préciser les étapes et les facteurs à prendre en compte aux fins d'une EFVP, sur le modèle du document de la CAI.

## 7. Notion de « renseignement sensible » (article 102 du Projet de loi)

Le Projet de loi insère la notion de renseignements sensibles notamment à ses articles 12 et 13 en définissant un renseignement comme étant « sensible » lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'atteinte raisonnable en matière de vie privée.

Nous sommes toutefois d'avis que cette définition ne semble pas aller assez loin en ce sens qu'il peut être confus pour les entreprises de déterminer dans chaque circonstance ce que constitue concrètement un renseignement sensible ou non. Par ailleurs, la définition telle que présentement rédigée dans le Projet de loi pourrait prêter à interprétation en ce sens que la sensibilité d'un renseignement pourrait être une notion subjective dans les situations moins flagrantes, et ce, pour le même renseignement. Comment les entreprises peuvent-elles lire dans les pensées des individus ?

À titre d'exemple, outre-Atlantique, le RGPD prévoit explicitement ce que constituent les données sensibles formant une catégorie particulière de données personnelles. En effet, l'article 9 du Règlement européen prévoit ce qui suit :

> *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.*

Ce type de données doit ainsi faire l'objet d'un traitement particulier explicitement mentionné dans le RGPD. Nous sommes d'avis qu'il serait pertinent d'intégrer ces mêmes précisions dans la Loi sur le secteur privé. Notre suggestion serait de s'inspirer des renseignements mentionnés à l'article 10 al. 1 de la *Charte des droits et libertés de la personne* qui dispose ce qui suit :

> *10. Toute personne a droit à la reconnaissance et à l'exercice, en pleine égalité, des droits et libertés de la personne, sans distinction, exclusion ou préférence fondée* ***sur la race, la couleur, le sexe, l'identité ou l'expression de genre, la grossesse,***

> ***<u>l'orientation sexuelle, l'état civil, l'âge</u>*** *sauf dans la mesure prévue par la loi,* ***<u>la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale, le handicap ou l'utilisation d'un moyen pour pallier ce handicap</u>****.*
> [Nos emphases et soulignements]

**Recommandation :**

20. Insérer dans la Loi sur le secteur privé une définition des renseignements personnels sensibles basée sur les critères établis dans l'article 10 de la Charte des droits et libertés.

## 8. Champ d'application territoriale de la Loi sur le secteur privé

Actuellement, la Loi sur le secteur privé ne définit pas son champ d'application territorial. Elle indique simplement que :

> *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*.

Le Projet de loi reste, lui aussi, muet quant au champ d'application territorial de la future loi.

Alors, comment déterminer le champ d'application territorial de la Loi sur le secteur privé, lorsqu'elle sera modifiée par le Projet de loi[40] ?

### 8.1 Application territoriale d'une loi en droit comparé

#### 8.1.1 La LPRPDÉ

Au niveau fédéral, l'article 4 de la LPRPDÉ prévoit que celle-ci s'applique aux organisations qui recueillent, utilisent et communiquent des renseignements personnels dans le cadre d'activités commerciales et aux entreprises fédérales qui font de même à l'égard de leurs employés. Toutefois, s'il ne donne aucune indication quant à la portée territoriale de la Loi, la jurisprudence s'en charge.

En effet, les tribunaux utilisent le critère du « lien réel et substantiel » pour déterminer si la LPRPDÉ s'applique aux organisations étrangères. En effet, la question permettant de savoir s'il y a lieu d'appliquer la LPRPDÉ à une organisation étrangère est « *l'existence entre le Canada et l'[activité] en question d'un lien suffisant pour que le Canada applique ses dispositions conformément aux "principes d'ordre et d'équité* »[41]. Par exemple, dans l'affaire *A.T.* c. *Globe24h.com*, la Cour fédérale a appliqué la

---

[40] Voir notamment Antoine GUILMAIN et Denis DOUVILLE, « The Québec Private Sector Privacy Act : When does it Apply to Organizations Outside of Québec? », (2019) 16-8 *Canadian Privacy Law Review*, p. 85 à 90; Antoine GUILMAIN et Éloïse GRATTON, « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », S.F.C.B.Q., vol. 465, *Développements récents en droit à la vie privée*, Cowansville, Éditions Yvon Blais, 2019, p. 67-134.

[41] *A.T.* c. *Globe24h.com*, 2017 FC 114.

LPRPDÉ à un Roumain qui exploitait un site Internet qui recueillait et publiait de la jurisprudence canadienne contenant des renseignements personnels. Même si le site Internet était exploité et hébergé en Roumanie, il contenait des décisions canadiennes, visait des Canadiens et avait des répercussions sur des Canadiens. La Cour fédérale a recouru à ces éléments pour établir un lien réel et substantiel avec le Canada[42].

#### 8.1.2 Le RGPD

Quant au Règlement européen général sur la protection des données (« RGPD »)[43], il définit son champ d'application territorial en son article 3, et ce de façon large « afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit » en vertu du RGPD[44].

Plus particulièrement, en vertu de son article 3, le RGPD s'applique tout d'abord à toute entité qui traite des données à caractère personnel et dont l'un de ses établissements est situé sur le territoire de l'UE, et ce, quel que soit le lieu où les données sont traitées[45].

Ensuite, l'article 3 du RGPD prévoit qu'il peut également s'appliquer à toute entité qui, bien qu'elle ne soit pas située sur le territoire de l'UE, vise (ou cible) le marché européen en (i) surveillant (ou en suivant) le comportement des individus situés sur le territoire de l'UE[46] ou (ii) offrant des biens/services (payants ou gratuits) aux particuliers situés dans l'UE[47].

De même, des lignes directrices du Comité européen à la protection des données[48] viennent expliquer comment appliquer le RGPD aux entreprises non situées sur le territoire de l'UE.

Au Québec, il n'existe rien de tel. Cette absence de clarification est une cause d'incertitude pour les entreprises.

### 8.2 Situation ambiguë au Québec

#### 8.2.1 État du droit

Le Projet de loi ne précise pas le champ d'application territorial de la Loi. Or, la Loi sur le secteur privé, dans sa rédaction actuelle, ne le fait pas non plus.

---

[42] *Id*.

[43] RGPD. Sur le champ d'application territorial du RGPD, voir notamment : Antoine GUILMAIN et Julie UZAN-NAULIN, « The territorial scope of private sector privacy laws : comparison Quebec - Canada- EU » (à paraître); Julie UZAN-NAULIN, « La portée (extra) territoriale du RGPD : le droit à l'oubli », dans Bulletin, *Fasken*, 28 novembre 2019, en ligne : < https://www.fasken.com/fr/knowledge/2019/11/the-extra-territorial-scope-of-the-gdpr >.

[44] RGPD, consid. 23.

[45] *Id*., art. 3 (1).

[46] *Id*., art. 3 (2)b).

[47] *Id.*, art. 3 (2)a).

[48] COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, « Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3) », version 2.0, 12 novembre 2019, en ligne : < https://edpb.europa.eu/sites /edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_fr.pdf >

En effet, la Loi sur le secteur privé dispose qu'elle s'applique à « *l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil* », selon lequel :

> *« 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 ».*

Ni la Loi sur le secteur privé, ni même le Code civil ne donnent d'indication sur le champ d'application territorial, mais pour que la Loi s'applique, selon la CAI, l'entreprise doit être exploitée au Québec[49].

Néanmoins, les tribunaux appliquent des facteurs généraux pour définir ce critère géographique. Dans l'affaire *Institut d'assurance du Canada* c. *Guay*[50], il a été considéré que la Loi s'appliquait à une entité située en Ontario qui vendait des biens et des services au Québec, même si l'entité n'avait qu'un bureau au Québec avec un nombre minimal d'employés qui n'étaient ni ses agents ni ses mandataires.

Les tribunaux ont également soutenu que les entreprises étrangères qui font affaire au Québec ou qui offrent des biens ou des services se retrouvant sur le marché québécois peuvent être des « entreprises » au sens de l'article 1525 du C.c.Q[51].

Toutefois, aucune approche précise, aucun test, n'a été développée pour préciser l'application de la Loi sur le secteur privé à une entreprise étrangère, ayant des activités au Québec, mais sans y avoir d'établissements[52].

### 8.2.2 Décision d'adéquation par l'UE

Le manque de clarté de la Loi sur le secteur privé quant à son champ d'application a été reproché par le Groupe de l'Article 29, prédécesseur du Comité Européen à la Protection des Données (« **CEPD** »)[53] quand la question de reconnaitre le Québec comme territoire adéquat a été posée. Parce que le Projet de loi ne définit pas le champ d'application territorial, les remarques ci-dessous trouvent toujours à s'appliquer.

C'est ainsi que le Groupe de l'Article 29 a recommandé de ne pas reconnaitre le caractère adéquat du Québec, notamment en raison de la divergence des positions prônées par l'État fédéral et la province quant au champ d'application territorial[54] :

---

[49] *Institut d'assurance du Canada* c. *Guay*, [1998] n° AZ-98031022, (C.A.I.).

[50] *Id*.

[51] *Serres Floraplus Inc*. c. *Norséco Inc*., 2008 QCCS 1455, par. 3 et 21.

[52] Antoine GUILMAIN et Éloïse GRATTON, « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », p. 71-76.

[53] Article 29 Working Group, « Opinion 7/2014 on the protection of personal data in Québec », WP 219, 2014.

[54] D'autres éléments ont également été pris en compte comme la nécessité de (i) renforcer les exigences de transparence concernant les personnes qui détiennent des renseignements personnels, (ii) définir le concept de " renseignements sensibles " et (iii) soumettre le transfert de renseignements à des dispositions contractuelles ou

*« En ce qui concerne le champ d'application territorial, la décision de la Commission européenne sur l'adéquation de la LPRPDÉ prévoit, entre autres, que "lorsqu'une province adopte une loi essentiellement similaire, les organisations, catégories d'organisations ou activités visées seront exemptées de l'application de la loi fédérale pour les transactions intraprovinciales ; la loi fédérale continuera de s'appliquer à toutes les utilisations et communications interprovinciales et internationales de renseignements personnels ainsi qu'à tous les cas où les provinces n'ont pas créé de loi similaire en tout ou en partie". Cette position est similaire à celle adoptée par le Commissariat à la protection de la vie privée du Canada.*

*Cependant, la CAI considère qu'en cas de transactions interprovinciales et internationales, la LPRPDÉ et la loi québécoise s'appliquent toutes deux. La CAI explique qu'au Canada, la loi constitutionnelle de 1867 organise le partage des compétences entre les gouvernements fédéral et provincial et que l'article 92(13) stipule que "dans chaque province, la législature peut exclusivement faire des lois relatives aux questions relevant [...] de la propriété et des droits civils dans la province". La CAI considère en outre que la notion de "propriété et droits civils dans la province" se réfère à toute relation entre des individus et comprend le droit à la protection de la vie privée qui englobe le droit à la protection des données personnelles. En effet, l'article 3 et les articles 35 à 41 du Code civil du Québec prévoient des règles sur la protection de la vie privée et des données.*

*De plus, la Loi du Québec précise qu'elle a pour objet d'établir " des règles particulières à l'égard des renseignements personnels concernant d'autres personnes qui recueillent, détiennent, utilisent ou communiquent à des tiers dans le cadre de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil" (article 1).*

*« En conclusion, les positions prônées par l'État fédéral et la province sur le champ d'application de la loi québécoise divergent. Si le Commissariat à la protection de la vie privée du Canada considère que la législation fédérale s'applique aux transferts tant interprovinciaux qu'internationaux des renseignements personnels, la CAI considère que la loi québécoise s'applique toujours aux situations internationales. Cette divergence d'interprétation entre le Commissariat à la protection de la vie privée du Canada et la CAI n'est pas nouvelle étant donné qu'en 2003, à la suite de l'adoption de la LPRPDÉ, la Cour d'appel du Québec a été saisie de la question de savoir si la compétence exclusive de la LPRPDÉ pour les entreprises fédérales était anticonstitutionnelle. À ce jour, la Cour d'appel du Québec n'a toujours pas statué. Le groupe de travail considère dès lors qu'il est nécessaire de clarifier le champ d'application territorial de la loi*

---

à d'autres dispositions législatives contraignantes afin d'assurer un niveau de protection des données comparable à celui qui prévaut dans l'UE.

> *québécoise avant que la Commission européenne n'apprécie si ce texte assure un niveau de protection adéquat* »[55].

Si, du point de vue constitutionnel, la position du Québec ne vise pas à amoindrir la portée de la loi, mais à l'élargir dès lors que deux lois s'appliquent (la LPRPDÉ et la Loi sur le secteur privé), il est important économiquement d'aller chercher cette reconnaissance d'adéquation en Europe. Cela permettrait un transfert de renseignements personnels de l'UE vers le Québec sans aucune autre formalité. L'étude plus approfondie du Projet de loi[56] montre que ce dernier tend à se rapprocher du RGPD. Il ne faudrait pas que l'adéquation ne soit pas reconnue en raison l'absence de précision quant au champ d'application territorial. N'oublions pas que c'est un des éléments qui a empêché une reconnaissance en 2014. Il ne faudrait pas retomber dans les mêmes travers.

C'est d'ailleurs ce qu'affirme le Groupe de l'Article 29 :

« *Le groupe de travail souligne que le champ d'application territorial la Loi sur le secteur privé du Québec en la relation avec la LPRPDÉ doit être clairement défini avant toute décision sur son adéquation prise par la Commission européenne* »[57].

**Recommandations :**

21. Clarifier le champ d'application territorial de la Loi sur le secteur privé de sorte que celle-ci soit applicable :

- à toute entreprise, québécoise, canadienne ou étrangère, ayant un établissement au Québec; et
- en l'absence d'établissement au Québec, à toute entreprise offrant des biens et/ou des services aux individus sur le territoire québécois.

---

[55] Article 29 Working Group, « Opinion 7/2014 on the protection of personal data in Québec », p.4 et ss.

[56] Julie UZAN-NAULIN, « Le PL 64: à la recherche du RGPD? », dans Bulletin, *Fasken*, 10 août 2020, en ligne : < https://www.fasken.com/fr/knowledge/projet-de-loi-64/2020/08/10-a-la-recherche-du-rgpd#:~:text=%20Le%20projet%20de%20loi%2064%20introduit%20%C3%A9galement,individu%20de%20recevoir%20les%20informations%20personnelles...%20More%20 >

[57] Article 29 Working Group, p. 17.

# Conclusion et résumé

Nous vous remercions sincèrement de l'opportunité qui nous a été offerte de faire nos représentations sur le Projet de loi. Nous espérons que nos commentaires vous permettront de vous aider et vous faire avancer dans vos travaux.

À titre de rappel, voici les recommandations que nous avons formulées :

**Communication des renseignements personnels à l'extérieur du Québec**

1. Introduire le principe d'imputabilité du responsable du traitement de renseignements personnels sans égard à l'emplacement des données et sans obligation pour une analyse de droit comparé[58].

2. Introduire des alternatives à la détermination de l'adéquation des juridictions étrangères, telles que des clauses contractuelles types ou des règles d'entreprise contraignantes, plus adaptées au commerce digital international ; et

3. Clarifier la notion d'« État ».

**Conséquences du non-respect des lois**

4. Restreindre les sanctions administratives à des contraventions pour des transgressions de nature plus technique et ayant moins d'impact sur la vie privée, afin d'éviter la création d'un système parallèle qui brouille les frontières entre régimes administratif et pénal.

5. Augmenter significativement l'écart entre les montants maximums pouvant être réclamés pénalement et civilement selon un ratio pouvant être de 1 pour 20, soit dans l'hypothèse d'une amende maximale de 25 000 000 $, d'une sanction maximale de 125 000 $, laquelle serait tout de même largement suffisante pour assurer un retour rapide à la conformité dans un processus administratif.

6. Étudier les conséquences d'inclure une référence aux articles 35 à 40 du *Code civil du Québec* dans l'article 93.1.

7. Revoir l'opportunité de prévoir un montant minimal pour les dommages-intérêts punitifs afin de laisser la discrétion requise aux tribunaux dans l'octroi des dommages appropriés.

---

[58] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel », Éditions OCDE, Paris, 2002, en ligne : < https://www.oecd-ilibrary.org/fr/science-and-technology/lignes-directrices-de-l-ocde-sur-la-protection-de-la-vie-privee-et-les-flux-transfrontieres-de-donnees-de-caractere-personnel_9789264296398-fr >.

### Portée de l’exemption de consentement en contexte de transaction commerciale

8. Élargir la définition de « transaction commerciale » pour y inclure des concepts de financement, de prêt, fusion et autres formes de réorganisation corporative n’impliquant pas nécessairement un « transfert de propriété de tout ou partie d’une entreprise ».

### La place du consentement

9. Retirer l’obligation de devoir demander un consentement « distinct » pour chacune des fins visées, mais plutôt viser un principe de clarté.
10. Réviser l’imposition de devoir mettre en place des politiques proportionnées à la nature et à l’importance des activités pour davantage mettre l’accent sur l’obligation de devoir mettre en place des politiques courtes, claires, concises et cohérentes.
11. Retirer l’obligation de devoir publier les politiques et pratiques internes d’une entreprise sur son site Internet ou par tout autre moyen approprié.
12. La Loi sur le secteur privé devrait expressément autoriser le consentement implicite et prévoir ses critères d’application.
13. La Loi sur le secteur privé devrait être modifiée afin de prévoir une exception à l’exigence de consentement en matière d’emploi, dans le même sens que les lois canadiennes sur la protection des renseignements personnels.

### Domaine de la recherche

14. Raccourcir au minimum possible le délai transitoire d’un an, suite à l’adoption du Projet de loi, pour l’entrée en vigueur des dispositions facilitant l’accès et l’utilisation des renseignements personnels à des fins d’étude, de recherche ou de statistique.
15. Valider avec le milieu scientifique que le processus proposé n’est pas inutilement complexe.
16. Ajuster et clarifier l’exigence de spécificité du consentement à obtenir, crucial notamment dans le secteur de la recherche médicale et des études cliniques.
17. Permettre une utilisation secondaire des renseignements personnels dans le même, voire plusieurs domaines thérapeutiques.

### Évaluation des facteurs relatifs à la vie privée

18. Circonscrire les cas où une EFVP devrait être réalisée, sur le modèle du RGPD, en cas de risque pour les droits et libertés des individus.

19. Préciser les étapes et les facteurs à prendre en compte aux fins d'une EFVP, sur le modèle du document de la CAI.

### Notion de « renseignements sensibles »

20. Insérer dans la Loi sur le secteur privé une définition des renseignements personnels sensibles basée sur les critères établis dans l'article 10 de la Charte des droits et libertés

### Champ d'application territorial de la Loi sur le secteur privé

21. Clarifier le champ d'application territorial de la Loi sur le secteur privé de sorte que celle-ci soit applicable :

- à toute entreprise, québécoise, canadienne ou étrangère, ayant un établissement au Québec; et
- en l'absence d'établissement au Québec, à toute entreprise offrant des biens et/ou des services aux individus sur le territoire québécois.

## AUTEURS

### Antoine Aylwin

Associé, Montréal | **Cochef national, vie privée et cybersécurité**
+1 514 397 5123 | aaylwin@fasken.com

La pratique d’Antoine est axée sur le litige administratif, civil et commercial, dont une partie importante est consacrée aux questions relatives à la protection des renseignements personnels dans les secteurs public et privé, la cybersécurité et les interventions en cas d’atteintes à la protection des données. Les clients font appel à Antoine pour son expertise dans ces domaines et pour ses conseils pratiques et opportuns sur les exigences en matière de conformité à la protection des renseignements personnels et lors d’incidents liés à la sécurité des données.

### Karl Delwaide

Associé, Montréal
+1 514 397 7563| kdelwaide@fasken.com

Karl Delwaide est reconnu comme avocat chevronné dans les domaines du droit public et de la protection de l’information et de la vie privée. Il est d’ailleurs l’un des fondateurs de ce groupe de pratique à l’échelle nationale du cabinet. Karl conseille des entreprises privées et des organismes publics, et les représente dans ces domaines, devant la Commission d’accès à l’information du Québec et d’autres tribunaux, y compris la Cour fédérale. Une importante partie de sa pratique est consacrée au droit administratif, réglementaire, disciplinaire et constitutionnel. Karl a été procureur pour le Gouvernement du Québec pendant de nombreuses années. Son expérience lui a permis de développer une solide expertise en matière de jugement déclaratoire, en injonction et contrôle judiciaire ainsi qu’en régulation économique.

## Jennifer Stoddart

Avocate, Montréal
+1 514 397 4367| jstoddart@fasken.com

Jennifer Stoddart est conseillère stratégique au sein du groupe Protection des renseignements confidentiels, vie privée et cybersécurité. Elle est reconnue comme étant une référence en matière de protection des renseignements personnels. Elle a occupé plusieurs postes à hautes responsabilités dans la fonction publique québécoise et canadienne. Jennifer a été Commissaire à la protection de la vie privée du Canada de 2003 à 2013. À ce titre, elle a supervisé de nombreuses enquêtes visant le monde virtuel, notamment celles concernant la politique de protection des renseignements personnels d'un site de réseautage social et les failles dans la sécurité des données d'un géant américain du commerce de détail. Auparavant, elle a été présidente de la Commission d'accès à l'information du Québec de 2000 à 2003 et, durant son mandat, la Commission a publié un rapport intitulé Une réforme de l'accès à l'information : le choix de la transparence. Ce dernier a mené à d'importants changements aux lois visant l'accès à l'information et la protection des renseignements personnels.

Elle a aussi occupé des fonctions aux Commissions canadienne et québécoise des droits de la personne.

## Julie Uzan-Naulin

Avocate, Montréal
+1 514 871 5967 | juzan@fasken.com

Membre du Barreau de Paris et du Barreau de Montréal et détentrice d'un doctorat en droit. Julie est spécialiste dans la protection des données, notamment du RGPD et de l'utilisation de cookies. Elle conseille les entreprises afin de s'assurer de leur conformité avec le RGPD et des autres lois sur la protection des renseignements personnels, notamment en préparant les documents requis en vertu du RGPD, comme les registres des activités de traitement et les études d'impacts. Elle est coauteure du Guide pratique Lamy Droit du Numérique pour les éditions 2017-2019.

## Guillaume Pelegrin

Avocat, Montréal
+1 514 397 7411 | gpelegrin@fasken.com

La pratique de Guillaume Pelegrin couvre tous les aspects du droit public et administratif. Il aide ses clients à atteindre la conformité dans des environnements réglementaires complexes, les assiste dans l'obtention des permis et autorisations et les représente en cas de litige devant tous les tribunaux pour des enjeux civils, administratifs, pénaux et d'expropriation.

## Aya Barbach

Avocate, Montréal
+1 514 397 7456 | abarbach@fasken.com

Aya exerce dans les domaines de la protection des renseignements personnels, de l'accès à l'information, de la cybersécurité et de la publicité et du marketing en ligne. Aya conseille autant les entreprises privées que les organismes publics dans tous les sujets reliés à la protection des renseignements personnels et de la vie privée. Elle aide les clients à élaborer et à mettre en œuvre des politiques et des procédures en matière de protection des renseignements personnels. De plus, Aya agit pour le compte de clients dans le cadre de demandes d'accès à l'information et de demandes de renseignements devant la Commission d'accès à l'information du Québec. Elle représente des clients devant divers tribunaux judiciaires et administratifs.

## William Deneault-Rouillard

Avocat, Montréal
+1 514 397 5113 | wdeneault@fasken.com

William est avocat spécialisé en droit de la protection des données personnelles et de la sécurité de l'information. William conseille des entreprises technologiques à forte croissance sur l'opérationnalisation de concepts tels que la protection de la vie privée et la sécurité de l'information dès la conception et ce dans une vaste gamme d'industries, dont les logiciels SAAS,le big data, l'Internet des objets (IoT), intelligence artificielle (AI), la neurotechologie, le blockchain et la cryptomonnaie. Il est fréquemment impliqué lors de la négociation et la rédaction d'ententes commerciales comportant des exigences à l'égard de la sécurité et de la protection des données. Il élabore également des politiques de protection de la vie privée.