CI– 026M
C.P. – PL 64
Protection des renseignements personnels

Commentaires sur le Projet de loi 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Par la Banque Canadienne Impériale de Commerce, la Banque de Montréal, la Banque Nationale, La Banque de Nouvelle-Écosse, la Banque Royale du Canada et La Banque Toronto-Dominion

Le 28 septembre 2020

Personne ressource :
Charles S. Morgan, Associé
McCarthy Tétrault SENCRL srl
cmorgan@mccarthy.ca

Mémoire présenté à la Commission des institutions de l'Assemblée nationale

Présentation des auteurs – Les Banques d'importance systémique intérieure au Canada (BISi)

Ce mémoire présente les commentaires et les recommandations des six banques suivantes quant aux dispositions du Projet de loi 64 : la Banque de Montréal, La Banque de Nouvelle-Écosse, la Banque Canadienne Impériale de Commerce, la Banque Nationale, la Banque Royale du Canada et La Banque Toronto-Dominion. Nous sommes désignées par le régulateur fédéral des institutions financières comme étant les six banques d'importance systémique intérieure nationale (« **BISi** »).

Avec la confiance de millions de Québécois et de Canadiens, les BISi ont une expérience unique quant aux enjeux liés à la protection des données de nos clients, qu'il s'agisse de particuliers ou d'entreprises. Nous protégeons les renseignements personnels et financiers les plus sensibles de nos clients. Nous avons aussi développé une expertise pointue sur la mise en œuvre des lois pour protéger les renseignements personnels tout en favorisant l'innovation et la promotion du secteur financier québécois. Nous avons le devoir de respecter le droit à la vie privée, tout en prenant les mesures nécessaires pour protéger les Québécois contre la cybercriminalité et d'autres formes de fraude.

Nous avons une expérience et une expertise considérables en matière de conformité aux lois applicables à la protection de la vie privée. Nos activités relèvent de la compétence fédérale, et en conséquence nous sommes assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques (*« **LPRDE** ») depuis son entrée en vigueur en 2001. Bien que les BISi relèvent du régime fédéral, chacune d'entre elles possède des filiales, telles des compagnies d'investissement et d'assurance, qui sont assujetties aux lois provinciales, dont notamment la *Loi sur la protection des renseignements personnels dans le secteur privé* (la « **Loi sur le secteur privé** »), ainsi qu'aux lois applicables au secteur privé en Alberta et en Colombie-Britannique. Nos services financiers sont offerts à des centaines de milliers de petites et moyennes entreprises partout au Canada. Nous sommes donc sensibles aux préoccupations des PMEs sur la question de la complexité engendrée par l'existence de plusieurs régimes règlementaires.

Les BISi participent activement aux travaux du Conseil sur l'auto-évaluation en matière de cybersécurité[1] du Bureau du surintendant des institutions financières (« **BSIF** ») et suivent les normes de la Ligne Directrice B-10 sur l'Impartition d'activités, de fonctions et de méthodes commerciales.[2] Elles participent ainsi aux évaluations, examens et conseils du BSIF sur les technologies de gestion du risque, notamment dans le cadre des consultations actuelles du BSIF relatives à l'initiative *Renforcer la résilience du secteur financier dans un monde numérique*.[3]

Pour les BISi, la résilience opérationnelle exige une collaboration avec des prestataires de services basés tant au Canada qu'ailleurs dans le monde en matière de lutte au blanchiment d'argent, de cybersécurité et de prévention de la fraude. Ces prestataires de

services doivent être sophistiqués et en mesure de protéger efficacement nos infrastructures, nos institutions et nos marchés dans un contexte technologique en constante évolution. Les malfaiteurs opèrent dans un environnement de plateformes mondialisé. Pour protéger nos concitoyens et nos clients, nous n'avons d'autre choix que d'adopter une approche globale.

Les BISi reconnaissent l'importance d'inspirer et de maintenir une confiance numérique grâce à des mécanismes transparents qui permettent à nos clients de conserver le contrôle sur leurs renseignements personnels et confidentiels.

L'expérience des BISi en matière de protection de la vie privée ne se limite pas à nos efforts de conformité au Canada. Chacune d'entre nous est également soumise à des régimes de juridictions étrangères, notamment le *Règlement général de protection des données* (le « **RGPD** ») *de l'Union européenne* (« **UE** ») et le *California Consumer Privacy Act* (« **CCPA** »). Les BISi adoptent – et même souvent établissent – les plus hauts standards de notre secteur d'activités en ce qui a trait à la protection des renseignements personnels, tant sur le plan national qu'international. Nous sommes des chefs de file dans la protection des données et nous occupons une position stratégique dans l'adoption de moyens d'échanges sécurisés des données en Amérique du Nord et dans le système financier mondial.

Résumé

Les six banques d'importance systémique intérieure canadiennes (BISi) apprécient l'opportunité de soumettre leurs observations à la Commission des institutions de l'Assemblée nationale relativement au Projet de loi 64 – *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (le « **Projet de loi 64** »). De plus, en tant que membres de l'Association des banquiers canadiens (« **ABC** »), nous tenons à indiquer que nous souscrivons aux commentaires distincts formulés par l'ABC dans son mémoire.

À cette occasion, nous suggérons certaines recommandations au gouvernement du Québec qui sauront, à notre avis, contribuer à faire de ce projet de loi un moteur du progrès économique et de l'innovation, y compris les suivantes :

1. Retirer les limites aux transferts de données à l'extérieur du Québec pour s'assurer de l'adéquation de la loi québécoise sur la protection des renseignements personnels avec la LPRDE à propos des flux de données transnationaux, suivant le principe de « responsabilité ».

2. Introduire des alternatives au consentement, comme la notion de « licéité du traitement » que l'on retrouve à l'article 6 du RGPD ou celle d'« activités d'affaires normales » du Ministère de l'Innovation des Sciences et du Développement économique (« **ISDE** »), afin d'éviter de lasser les consommateurs avec de multiples demandes de consentement.

3. Assurer l'alignement et la cohérence entre les lois de protection de la vie privée au Canada.

4. Établir un seuil de gravité, prenant en compte le risque et le contexte, afin de déterminer si une analyse d'impact des facteurs relatifs à la vie privée est justifiée. Ce modèle devrait être conforme aux dispositions de l'article 35 du RGPD, et applicable lorsque le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

5. Prévoir une certaine forme de coordination multi-juridictionnelle des sanctions par les régulateurs, afin d'éviter qu'une organisation soit sanctionnée de manière disproportionnée ou à de multiples reprises en lien avec le même incident. Ce cadre devrait inclure un montant d'amendes globales maximum.

6. S'assurer que les lois québécoises de protection de la vie privée concernant le droit de retrait (opt-out) du profilage et du traitement automatisé comprennent des définitions précises et des exemptions pour faire en sorte qu'elles n'affectent pas par inadvertance ou n'interdisent pas des activités bénéfiques et qu'elles n'obligent pas la divulgation d'informations commerciales confidentielles.

7. S'assurer que le Projet de loi 64 évite les conséquences non anticipées et indésirables qui sont survenues lors de la mise en œuvre du RGPD, tout en établissant les bases pour l'obtention du statut d'adéquation pour faciliter les flux de données entre l'UE et le Québec.

Commentaires sur le Projet de loi 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Le Projet de loi 64 représente l'occasion pour le gouvernement du Québec d'être de nouveau à l'avant-garde en matière de lois sur la protection de la vie privée et des renseignements personnels au Canada. De telles lois doivent être rédigées avec précaution. Nous présentons plus bas plusieurs observations et recommandations dans le but d'aider le gouvernement du Québec à trouver le juste équilibre pour sa nouvelle loi, un équilibre qui protégerait adéquatement les renseignements personnels des citoyens tout en alimentant le progrès économique et l'innovation.

Le Québec est depuis longtemps un chef de file

Le Québec est depuis plusieurs années un chef de file en matière de protection de la vie privée. En 1993, le Québec présentait la Loi sur le secteur privé, premier régime de protection des renseignements personnels en Amérique du Nord. Ce n'est qu'à compter de l'an 2000 que le reste du Canada s'est mis au diapason, lorsque le gouvernement fédéral a finalement adopté la LPRDE. Seules la Colombie-Britannique et l'Alberta ont à ce jour emboité le pas et adopté leurs propres régimes de protection des renseignements personnels dans le secteur privé (tous deux intitulés *Personal Information Protection Act*).

Le Québec sera à nouveau chef de file au Canada, étant le premier gouvernement à proposer la prochaine génération de régimes sur la protection de la vie privée avec son Projet de loi 64. Cette fois-ci, le Québec n'est pas le seul à manifester son intention de moderniser la législation sur la protection de la vie privée à l'ère numérique. Le gouvernement du Canada a aussi entrepris de vastes consultations et entend proposer des réformes à la LPRDE. L'Ontario mène également une consultation dans l'objectif d'adopter son propre régime de protection des renseignements personnels. Un comité spécial fait une révision du *Personal Information Protection Act* de la Colombie-Britannique. Ils ont tenu des audiences publiques et plusieurs mémoires ont été déposés.

Les avantages pour les consommateurs et les petites et moyennes entreprises (« PMEs »)

Les données peuvent constituer un outil puissant pour favoriser une croissance économique durable. La manière dont les législateurs abordent la question de la protection des renseignements personnels tout en cherchant un juste équilibre avec l'utilisation et la valeur des informations qui peuvent être tirées des données lorsque celles-ci sont suffisamment dissociées des renseignements personnels et nominaux, aura un impact direct sur la capacité des institutions québécoises et canadiennes de favoriser la recherche et l'innovation.

Les consommateurs veulent une approche sécuritaire et simple lorsqu'ils font des transactions. Les commerçants, tout particulièrement les PMEs, veulent faire la transition d'une offre de service traditionnelle à un mode de vente en ligne, dans un espace de commerce qui est de plus en plus numérique. Ceci offre des avantages autant pour les

consommateurs que pour les PMEs, toutefois cela exige une juste combinaison de sécurité et d'accessibilité. Une étude approfondie des effets et impacts des nouveaux droits de protection des données et des droits à la vie privée avant leur adoption permettra d'obtenir une bonne lecture de l'impact économique des mesures proposées en tenant compte de la confiance nécessaire des consommateurs et des entreprises.

Il est essentiel que le citoyen soit au centre d'un régime de protection des renseignements personnels, ce qui requiert des consentements que les consommateurs puissent être en mesure de comprendre, tout en évitant des demandes multiples qui mènent à ce qui est communément reconnu comme le « *consent fatigue* ». Nous savons par l'expérience acquise en travaillant avec nos PMEs que celles-ci investissent des sommes considérables en frais juridiques et de consultants afin de mettre en place des mesures conformes aux exigences règlementaires qui s'appliquent à leurs entreprises, incluant les règles de conformité. Le Projet de loi 64 aurait pour effet d'appliquer un régime de protection des renseignements personnels complexe à toutes les PMEs. Non seulement les gouvernements doivent tenir compte des coûts associés aux nouvelles exigences, mais ils doivent aussi tenir compte des graves pénuries de main-d'œuvre dans l'embauche de professionnels œuvrant dans le domaine.

Nous favorisons la protection des données et des droits à la vie privée des Québécois et des Canadiens en proposant une approche réglementaire équilibrée, alignée et cohérente qui favorise le caractère dynamique, compétitif et novateur du secteur financier.

Une approche adaptée à l'ère numérique

Nous appuyons le Québec dans son leadership pour faire avancer les lois sur la protection des renseignements personnels au Canada. Nous sommes confiants que le Québec a toutes les ressources nécessaires et la capacité de répondre aux défis liés à la protection des données personnelles et confidentielles dans le contexte d'une économie numérique mondialisée.

Le Québec en 1993 pouvait agir seul. En 2020, cela pose des défis considérables. Les enjeux liés aux données et à la protection de la vie privée transcendent les frontières nationales, tout autant que les outils innovateurs essentiels à la protection des Québécois et des Canadiens contre la cybercriminalité et d'autres formes de fraude.

La meilleure façon de protéger les citoyens et de placer le Québec à l'avant-plan de l'économie de l'innovation est de mettre son leadership au service de la promotion d'un régime robuste, cohérent et efficace de lois sur la protection des renseignements personnels qui encouragent la gestion responsable et sécurisée des données à travers tout le Canada. Le Canada pourrait ainsi devenir un leader mondial dans le juste équilibre entre la protection des données et l'innovation de nos entreprises. Nous souhaitons que le Québec interpelle ses homologues fédéraux et provinciaux dans la mise sur pied d'un régime uniforme, efficace et innovant.

Le Québec et le Canada participent à une économie mondialisée, notamment par une structure internationale de données. Un régime cohérent de protection des renseignements personnels et de protection des données doit également être aligné avec les législations internationales d'importance telles que le RGPD et le CCPA. Les nouvelles lois ont pour vocation d'assurer un plus grand contrôle aux individus par rapport à la cueillette et l'utilisation de leurs renseignements personnels.

Le Québec et le Canada peuvent en parallèle bénéficier des leçons apprises dans le contexte où l'application des dispositions du RGPD et du CCPA a produit certains effets non désirés. Il faut à tout prix éviter de reprendre à notre compte des normes étrangères qui ont entrainé de la confusion chez les consommateurs sur des enjeux liés au consentement, ou encore de lourds fardeaux pour les petites entreprises et/ou la perturbation des flux de données qui protègent les consommateurs ou leur permettent d'accéder à des services innovants. L'amélioration des régimes internationaux de protection existants conférera au Québec et au Canada un avantage concurrentiel dans l'économie mondiale.

Bien que nous discutons de ces enjeux plus en détails dans notre mémoire, vous trouverez ci-après certaines recommandations pour la mise sur pied d'un régime équilibré, aligné et cohérent :

- **Des exigences simplifiées en matière de consentement** : Les exigences quant au consentement prévues dans le Projet de loi 64 pourraient être ajustées afin de les rendre compatibles avec les normes internationales. Le consentement explicite nous apparaît opportun lorsque des renseignements sensibles sont recueillis, lorsque l'utilisation envisagée des renseignements recueillis n'est pas conforme aux attentes légitimes des individus concernés ou lorsqu'un risque particulier est présent. Le consentement explicite ne devrait pas être utilisé en toutes circonstances. La notion de licéité du traitement (« legitimate interest ») que l'on retrouve dans le RGPD ou la proposition du ISDE en lien avec les activités d'affaires normales sont des alternatives intéressantes fondées sur le principe du consentement donné pour une ou plusieurs finalités spécifiques. Une telle approche permet de respecter les attentes des clients tout en évitant de les interpeller à répétition avec de multiples demandes de consentement (ce qui mène à un phénomène de « consent fatigue »).

- **Une approche centrée sur la responsabilité pour les données transfrontalières :** Le Québec et les autres provinces pourraient privilégier une approche flexible centrée sur le principe de responsabilité énoncé à la LPRDE concernant le transfert de renseignements personnels à l'extérieur du Canada. L'approche de la LPRDE est bien comprise, notamment en raison des efforts du Commissaire à la protection de la vie privée du Canada pour déterminer à quels moments il est approprié de transférer des renseignements personnels hors du pays et quelles mesures de protection devraient être mises en place. À ce jour, cela s'est révélé être une approche efficace pour protéger les renseignements personnels tout en permettant aux entreprises canadiennes d'utiliser des outils de premier niveau, incluant des outils de cybersécurité qui hébergent des renseignements à l'extérieur du Canada. Reconnaissant l'importance économique des mouvements transnationaux de données, les BISi souhaitent la mise en place d'un régime équilibré, aligné et cohérent des règles de transfert des données à l'intérieur du Canada. Ainsi, comme tout le Canada bénéficierait de protections statutaires substantiellement similaires et cohérentes, les modifications proposées sur les transferts transfrontaliers de renseignements personnels dans le Projet de loi 64 pourraient être supprimées dans la mesure où elles s'appliquent aux transferts à l'intérieur du Canada.

- **Mécanisme d'application renforcé et équitable** : Les BISi reconnaissent que le non-respect des lois doit entrainer des pénalités suffisamment élevées pour

susciter des changements de comportements. Cependant, des sanctions trop sévères sont susceptibles d'entrainer des réactions et des comportements qui décourageront l'innovation. Des sanctions perçues comme étant trop sévères risquent d'inciter des entreprises à offrir aux Québécois des versions moins optimales de leurs services par crainte de contrevenir aux dispositions complexes du Projet de loi 64. Cela réduirait l'offre de service aux consommateurs et aux entreprises. Dans un système caractérisé par l'équité procédurale, les sanctions doivent être justes et proportionnelles. Le Québec devrait être prudent et éviter d'adopter un régime qui pourrait mener à une multiplication des sanctions pour un même événement.

- **Droit de se soustraire au profilage non systématisé :** Le Projet de loi 64 prévoit une définition trop large du profilage. La définition proposée semble bien adaptée dans le contexte du profilage en ligne par des tierces parties cherchant à effectuer des campagnes de marketing. Par contre, telles que rédigées, les dispositions concernées pourraient aussi viser des analyses de données réalisées dans le cours normal des affaires et qui nécessitent un ensemble de données suffisamment complet dans le but de mieux servir la clientèle, gérer les risques, prévenir la fraude ou lutter contre le blanchiment d'argent. Il y a lieu de s'assurer que les dispositions de la Loi sur le secteur privé relatives au droit de se soustraire au profilage ne fassent pas perdre des avantages aux clients et qu'elles soient harmonisées avec la LPRDE. L'exclusion des données relatives à des clients qui se seraient retirés risque de fausser les résultats analytiques.

- **Meilleure protection uniformisée pour les Québécois et les Canadiens** : Le Projet de loi 64 comprend un certain nombre de changements qui devraient être adoptés uniformément dans l'ensemble du Canada, comme l'exigence que les organisations se dotent d'un cadre de gouvernance pour la protection des renseignements personnels, une norme que les BISi appliquent depuis plusieurs années. Le Québec devrait promouvoir l'adoption de ces changements par les législateurs fédéral et provinciaux. De cette façon, nous pourrions éviter l'exemple des États-Unis, où une mosaïque de lois sectorielles et étatiques a entrainé des coûts réglementaires importants. Cela a aussi pour effet de perturber la participation des petites entreprises à l'économie nationale et détourne des ressources précieuses qui pourraient être mises au profit de l'amélioration de la transparence et de l'innovation.

- **Évaluation contextuelle du risque** : Dans une économie basée sur l'innovation, il est primordial de s'assurer que les entreprises québécoises aient accès à des données justes, utiles et pertinentes, ce qui inclut selon les conditions fixées par le législateur, les renseignements personnels de leurs clients. Ainsi, elles seront en mesure de développer des produits concurrentiels et des services pour leurs clients locaux et internationaux. Les BISi reconnaissent les opportunités, mais également les risques potentiels associés aux méthodes d'analyse de données. Les efforts pour protéger les consommateurs et les entreprises contre ces risques doivent être faits selon une méthodologie adaptée au contexte local pour éviter d'étouffer l'innovation. Toute réglementation du traitement des données devrait établir des critères prenant en compte la sensibilité des données et le niveau de risque relié au traitement de celles-ci.

Ci-dessous, nous présentons nos commentaires détaillés sur les enjeux les plus pressants du Projet de loi 64. Nous avons inclus des sources et des références externes qui permettront de mieux mesurer les répercussions complexes des choix à faire pour mener le Québec et le Canada vers une nouvelle ère de protection de la vie privée et de protection des données. Nous sommes disponibles pour soutenir la Commission et le gouvernement du Québec dans leur recherche de solutions face à ces enjeux complexes. Nous souhaitons la création d'un régime québécois de protection de la vie privée efficace qui s'arrimerait avec les autres régimes et qui pourrait devenir un modèle à l'échelle mondiale.

Analyse détaillée du Projet de loi 64 et Recommandations

1. Restrictions au transfert de données à l'extérieur du Québec

Article 103. Le Projet de loi 64 exige des organisations qu'elles procèdent à une évaluation des facteurs relatifs à la vie privée avant de communiquer un renseignement personnel à l'extérieur du Québec. Le Projet de loi 64 prévoit que les organisations pourront communiquer des renseignements à l'extérieur du Québec uniquement lorsque cette évaluation démontre que :

1. Le renseignement bénéficierait, dans la juridiction de destination, d'une protection équivalente à celle dont il dispose au Québec; et

2. L'organisation conclut avec l'entité à qui l'information est communiquée un accord écrit qui tient compte de l'évaluation et, le cas échéant, qui prévoit les modalités convenues pour atténuer les risques identifiés.

Commentaires

Les restrictions imposées par le Projet de loi 64 au transfert des données à l'extérieur du Québec ne sont pas au diapason de la **LPRDE**[4] ou les *Personal Information Privacy Act* (« **PIPA** ») de la Colombie-Britannique[5] et de l'Alberta[6], lesquels n'imposent pas de règles normatives sur les flux transnationaux de données, mais précisent plutôt que les organisations sont responsables de la protection des renseignements personnels confiés à une tierce partie. Les organisations sont tenues d'assurer, par voie contractuelle, un degré comparable de protection.[7] Le critère d'« équivalence » que l'on retrouve au Projet de loi 64 est plus élevé que l'exigence d'« adéquation » prévue au RGPD.[8] Lorsque le critère d'adéquation n'est pas rencontré dans la juridiction de destination, le Projet de loi 64 ne prévoit pas de mécanisme alternatif, contrairement au RGPD qui inclut des mécanismes pour l'obtention de garanties appropriées par voie de clauses contractuelles standards et en s'appuyant sur des règles d'entreprise contraignantes.

Les restrictions envisagées par le Projet de loi 64 entrainent des conséquences négatives pour les consommateurs québécois et créent des défis opérationnels majeurs pour les BISi.[9] L'exigence d'équivalence est susceptible de grandement limiter la capacité des BISi à transférer les renseignements personnels de leurs clients et employés à l'extérieur du Québec. Les BISi seraient donc limitées dans leur capacité à développer les meilleures pratiques commerciales et ententes avec des fournisseurs, dans leurs activités de détection de la fraude, de gestion et de prévention des risques liés à la cybersécurité ainsi que dans leurs efforts de conformité et de prévention eu égard au blanchiment d'argent.[10] Dans une étude publiée en 2019, l'*Institute of International Finance* examine les lois sur la localisation des données de différents pays et conclut que les restrictions aux mouvements transnationaux de données affectent négativement les systèmes financiers et l'économie en général, notamment en augmentant la complexité des TI et des données. Ce faisant, elles nuisent à la gestion des risques, aux enjeux liés à la cybersécurité et aux efforts en matière de lutte contre le blanchiment d'argent des institutions financières. Ces restrictions réduisent également l'accès aux services financiers et aux marchés dans certains pays.[11]

Si le critère d'équivalence empêchait les BISi de faire affaires avec les fournisseurs de services internationaux, d'une part, la sécurité, l'innovation et l'efficacité risquent fort probablement d'être affectées et d'autre part, les consommateurs risquent de devoir faire face à une diminution des choix des produits et services bancaires.[12]

De plus, l'exigence d'équivalence préconisée par le Projet de loi 64 apparaît contraire aux obligations du Canada en matière de transferts internationaux de données prévus par divers accords commerciaux dont le Canada est partie, tout particulièrement l'Accord de partenariat transpacifique global et progressiste (« **PTPGP** »)[13] et l'Accord Canada-États-Unis-Mexique (« **ACEUM** »).[14] Vu son caractère restrictif et en l'absence d'une alternative à l'exigence « d'équivalence », cette règle est susceptible d'être interprétée comme restreignant indûment le mouvement des données pour des raisons commerciales en contravention des dispositions de l'article 14.11 PTPGP et de l'article 19.11 ACEUM. De plus, l'exigence « d'équivalence » risque de devenir une exigence *de facto* pour les entreprises de posséder des infrastructures informatiques à l'intérieur du Québec, une exigence en totale contradiction des prescriptions de l'article 14.13 du PTPGP et de l'article 19.12 de l'ACEUM.

Par ailleurs, il est à noter qu'en vertu du RGPD, il revient à un groupe de travail composé de régulateurs qualifiés de procéder à l'évaluation de l'« adéquation » des lois étrangères de protection des données. Or, le Projet de loi 64 impose cette responsabilité à des entreprises qui n'ont pas les ressources ou l'expertise nécessaires pour effectuer ce genre d'évaluation, notamment les PMEs.

Enfin, bien qu'une liste de juridictions dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec sera publiée dans la Gazette officielle du Québec, il n'est pas, à ce jour, possible de savoir si la LPRDE, le PIPA de la Colombie-Britannique et le PIPA de l'Alberta seront jugés adéquats.

> **Recommandation #1:** Retirer les limites aux transferts de données à l'extérieur du Québec pour s'assurer de l'adéquation de la loi québécoise sur la protection des renseignements personnels avec la LPRDE à propos des flux de données transnationaux, suivant le principe de « responsabilité ».

2. Exigences de consentement

Article 102. Le Projet de loi 64 exige que le consentement soit demandé pour chacune des fins spécifiques pour lesquelles il est donné « en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. » Le Projet de loi 64 exige également que, pour les mineurs âgés de moins de 14 ans, le consentement soit obtenu de la personne qui bénéficie de l'autorité parentale.

Article 102. Le Projet de loi 64 exige un consentement manifesté de façon expresse lorsqu'il s'agit de renseignements personnels sensibles. Un renseignement est considéré comme sensible si, en raison de sa nature ou du contexte de son usage ou de sa communication, il suscite un haut degré d'atteinte raisonnable en matière de vie privée.

Article 111. Le Projet de loi 64 inclut une nouvelle obligation d'informer la personne de son droit de retirer son consentement.

Commentaires

Les exigences strictes du Projet de loi 64 relativement au consentement risquent de nuire aux mouvements de données dans le contexte d'une économie moderne.[15] Elles sont également incompatibles avec les objectifs proposés par l'ISDE de simplifier les exigences en matière de consentement sous la LPRDE et de garantir aux individus un contrôle accru sur leurs données sans créer de répétitions contraignantes.[16] En raison des lourdes exigences du Projet de loi 64, les consommateurs pourraient se voir interpelés à répétition et voir leur temps monopolisé par de multiples demandes d'obtention de consentement.[17]

Les nouvelles exigences quant au consentement devraient être clarifiées. La signification des termes « distinctement de toute autre information communiquée à la personne concernée » demeure ambiguë. Il en va de même des types de renseignements qui doivent être considérés comme « sensibles » en raison de la définition circulaire contenue à l'article 12 du Projet de loi 64. La définition pourrait être plus spécifique et prévoir le traitement qui doit être accordé à des catégories spécifiques de données, comme c'est le cas à l'article 9 du RGPD. La lecture de ces exigences semble suggérer que les BISi devraient retirer les clauses de consentement des demandes, conventions et autres documents similaires afin de fournir un formulaire de consentement séparé, ce qui est complexe, particulièrement pour les PMEs, et nécessiterait pour les clients une étape additionnelle de révision de documents.[18]

De plus, le Projet de loi 64 ne contient aucune exception en ce qui a trait au consentement des employés, compliquant l'administration de la relation employeur/employé en raison du déséquilibre systémique entre ceux-ci, lequel rend presque impossible l'obtention d'un « consentement libre et éclairé ».

Finalement, l'obligation d'informer une personne de son droit de retirer son consentement est problématique dans les situations où les informations demandées sont essentielles à la prestation des services.

> **Recommandation #2 :** Simplifier les exigences de consentement du Projet de loi 64 de manière pratique, en fonction de principes qui les rendent compatibles avec les exigences en matière de consentement qui sont présentes dans la LPRDE, notamment en retirant les exigences pour un consentement spécifique et détaillé pour chaque usage spécifique.
>
> **Recommandation #3 :** Clarifier les circonstances pour lesquelles le consentement manifesté de manière expresse est requis ou non.

Recommandation #4 : Introduire des alternatives au consentement, comme la notion de « licéité du traitement » que l'on trouve à l'article 6 du RGPD ou celle d'« activités d'affaires normales » du Ministère de l'Innovation des Sciences et du Développement économique (« **ISDE** »), afin d'éviter de lasser les consommateurs avec de multiples demandes de consentement.[19]

3. Un régime de protection de la vie privée aligné et cohérent

Commentaires

L'industrie bancaire est préoccupée par tout changement aux régimes législatifs provinciaux et fédéral de protection de la vie privée qui entraine l'existence d'exigences normatives distinctes d'un régime à l'autre, provoquant un manque d'uniformité et de cohérence.

Les BISi ainsi que d'autres entreprises nationales et internationales opèrent et fournissent des produits et des services aux consommateurs canadiens à travers le Canada. La LPRDE régit les activités des BISi en raison du fait que les activités bancaires tombent sous la catégorie des ouvrages et entreprises fédérales. Inversement, les activités des filiales des BISi (telles que leurs filiales d'assurances et d'investissements) sont assujetties aux lois provinciales de protection de la vie privée au Québec, en Alberta et en Colombie-Britannique, et à la LPRDE dans les autres provinces.

Le fait d'être régis par des normes et règlements en matière de protection de la vie privée en leur essence similaires à l'échelle nationale permet aux Canadiens de bénéficier d'un ensemble de protections claires, uniformes et cohérentes (ex : communication restreinte et consentement éclairé), qui ne dépendent pas des produits qu'ils détiennent, des services qu'ils reçoivent ou de leur province d'appartenance.[20] Des règles uniformes et cohérentes en matière de vie privée assurent une meilleure compréhension des Canadiens de leurs droits liés à la protection de la vie privée. Assurer le maintien de l'uniformité et de la cohérence entre les exigences provinciales et fédérales en matière de protection de la vie privée faciliterait les opérations transfrontalières et les efforts de conformité, en plus de permettre aux organisations de fournir des produits et des services innovateurs, et ce, au bénéfice de tous les Canadiens.

Le manque d'alignement et de cohérence du Projet de loi 64 avec les normes nationales et internationales n'est pas au diapason des tendances globales actuelles. En particulier, reconnaissant l'importance économique des mouvements transnationaux efficaces de données, un nombre croissant d'initiatives sont mises en œuvre pour assurer l'uniformité non seulement à l'intérieur des états, mais aussi à l'échelle internationale (tel qu'en fait foi le RGPD).

Les impacts contre-productifs d'un échec en matière d'uniformisation et de cohérence sont nombreux et connus.

Par exemple, aux États-Unis, le fouillis que représentent les lois sur la vie privée uniques à chaque État et spécifiques à certains secteurs d'activités a été décrit par la Chambre de Commerce des États-Unis comme un « carambolage de 50 voitures » qui impose d'énormes coûts opérationnels et légaux sans garantir des bénéfices publics proportionnels.[21]

Le manque d'uniformité entre les juridictions est aussi extrêmement onéreux. Le Département californien de la Justice a déclenché une évaluation détaillée des coûts liés à la conformité au *California Consumer Privacy Act* (« **CCPA** »). Ce rapport a conclu que le « coût total de la conformité initiale avec le CCPA est d'environ 55 milliards $, soit l'équivalent d'environ 1.8% du produit intérieur brut de la Californie en 2018 ».[22] En Californie, les avantages pour les consommateurs se sont avérés négligeables, comparativement au ratio coût-bénéfice de 14:1 initialement estimé par le ministère de la Justice de la Californie suite à l'adoption du CCPA.[23] Les entreprises de la Californie ont été obligées d'absorber ces coûts, en plus des autres coûts associés à la présence des normes différentes et en constante évolution qui sont appliquées par d'autres états. Ces disparités coûteuses entre les normes de protection de la vie privée ont poussé de nombreux intervenants à souhaiter l'établissement d'une norme nationale commune pour favoriser l'innovation et pour maintenir la position des États-Unis en tant que leader dans le domaine des technologies.[24]

Le manque d'alignement du Projet de loi 64 lorsque comparé aux autres lois canadiennes de protection de la vie privée est préoccupant. En effet, des études économiques ont documenté la façon dont les coûts de conformité augmentent de façon significative en raison de lois sur la protection de la vie privée plus normatives et punitives, qui n'offrent pourtant pas davantage de bénéfices pour les consommateurs. De telles exigences entrainent des coûts considérables, même dans un environnement aligné et cohérent. La *Information Technology and Innovation Foundation* (« **ITIF** ») a récemment publié une étude détaillée qui concluait que si le Congrès américain adoptait une loi qui reprenait plusieurs des dispositions centrales du RGPD ou du CCPA, le coût pour l'économie américaine serait d'environ 122 milliards $, ou 483 $ par adulte vivant aux États-Unis, par année, représentant plus de 50% de ce que les citoyens américains dépensent pour leurs factures d'électricité chaque année. En revanche, si le Congrès adoptait plutôt un ensemble plus ciblé de mesures de protection de la vie privée, la protection des consommateurs serait accrue, mais à un coût réduit de 95%, soit environ 6.5 milliards $ par année.[25]

Enfin, la sévérité d'un régime de protection de la vie privée ne favorise et ne coexiste pas nécessairement avec la sécurité de l'information. De nombreuses études ont identifié plusieurs effets négatifs importants sur la sécurité résultant de l'adoption du RGPD. Ceux-ci incluent la mise en place de mesures de recherche sur la sécurité défensive via le blocage d'information publique sur la base de données de protocole Internet WHOIS, une augmentation du nombre de vols d'identité grâce au détournement des droits d'accès, des réticences à l'utilisation d'outils de vérification de l'identité et la diminution de la qualité des ensembles de données qui sont nécessaires pour la détection de cyberattaques.[26]

Recommandation #5 : Assurer l'alignement et la cohérence entre les lois de protection de la vie privée au Canada.

Recommandation #6 : Le Québec pourrait prendre avantage de son leadership afin de créer un groupe de travail composé de ministres fédéraux et provinciaux pour discuter d'un régime réglementaire coopératif et unifié de protection de la vie privée pour l'ensemble du Canada.

Recommandation #7 : Le régime modernisé de protection de la vie privée devrait être conçu afin d'obtenir une décision d'adéquation favorable de la part des régulateurs de l'UE dans le but de favoriser les mouvements de données entre l'UE et le Canada, tout en atténuant certains des aspects excessivement sévères du RGPD qui ont entrainé des conséquences négatives. À ce propos, le maintien de notre statut de conformité favorable servira également à maintenir notre avantage concurrentiel par rapport aux États-Unis relativement aux transferts de données de l'UE.

4. Nécessité d'une évaluation du risque plus contextuelle

Article 100. Le Projet de loi 64 va beaucoup plus loin que l'approche connue sous le nom de « privacy-by-design ».[27] Il adopte plutôt une approche de « confidentialité par défaut » suivant laquelle une organisation qui recueille des renseignements personnels en offrant un produit ou un service technologique devra s'assurer que les paramètres de ce produit ou de ce service assurent, par défaut, le « plus haut niveau de confidentialité », et ce, sans que la personne concernée n'ait à intervenir.

Commentaires

Les mesures proposées s'écartent de l'approche actuellement préconisée en matière de protection des renseignements personnels qui se fonde sur l'évaluation du risque. Cette approche est particulièrement pertinente puisqu'elle permet de concentrer les efforts des organisations sur la protection des renseignements dans les cas où il existe un risque élevé de préjudice pour les individus en cas d'utilisation inappropriée de ces renseignements.[28]

Contrairement au RGPD qui exige que les organisations prennent des mesures technologiques et administratives appropriées,[29] le Projet de loi 64 leur impose une obligation, sans réserve, de mettre en place « le plus haut niveau de confidentialité » par défaut. Imposer une telle obligation par défaut et sans égard aux facteurs prévus par le RGPD, soit : l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que le degré de probabilité et de gravité des risques, entraine d'importants coûts pour les organisations. Puisque le RGPD adopte une approche contextuelle et flexible, une incapacité opérationnelle à fournir un niveau élevé de confidentialité par défaut ne constituerait pas automatiquement une violation de la règlementation, par exemple dans un cas où il y a absence de risque réel de préjudice grave. L'approche du Projet de loi 64 laisse place à une interprétation suivant laquelle l'absence du « plus haut niveau de confidentialité » par défaut constitue automatiquement une violation de la loi, et ce, même dans une situation à faible risque ou

sans risque. Un tel résultat pourrait entrainer des coûts inutiles pour les organisations et priver les consommateurs d'une expérience client conforme à leurs attentes et prenant en compte le risque applicable à différentes situations.

La section du Projet de loi 64 portant sur les analyses d'impact des facteurs relatifs à la vie privée (« **AI** ») ne prévoit aucun seuil de gravité contrairement à ce qui est prévu dans le RGPD. Dans sa mouture actuelle, le Projet loi 64 exigerait qu'une AI soit effectuée dans le cadre de presque toutes les activités des entreprises, sans égard au niveau de risque. L'article 95 du Projet de loi 64 prévoit l'ajout d'une exigence à l'effet que : « 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. »

L'approche prévue à l'article 35 du RGPD protège les consommateurs en exigeant une AI préalablement au lancement d'un produit ou d'un service à risque élevé. Cette approche prend en considération le fardeau qui serait imposé aux entreprises de toute taille si chaque initiative devait requérir une AI, indépendamment du risque. L'article 35 prend également en compte le contexte de chaque situation en demandant aux organisations de considérer la nature, l'étendue et l'objectif du traitement pour déterminer si une AI est nécessaire.

Finalement, la norme du « plus haut niveau de confidentialité » manque de clarté quant à sa nature et sa portée. Ce manque de clarté peut entrainer des difficultés en obligeant les organisations à imposer des niveaux de protection disproportionnés à des données non sensibles (ce qui aurait pour effet d'imposer des obstacles aux clients qui désirent accéder à ces données).

Recommandation #8 : Modifier l'approche du « plus haut niveau de confidentialité » par défaut et favoriser plutôt l'approche acceptée par la communauté internationale de « privacy by design/privacy by default » afin d'assurer une uniformité entre la loi québécoise et l'approche développée au Canada et adoptée dans le RGPD.

Recommandation #9 : Établir un seuil de gravité, prenant en compte le risque et le contexte, afin de déterminer si une analyse d'impact des facteurs relatifs à la vie privée est justifiée. Ce modèle devrait être conforme aux dispositions de l'article 35 du RGPD, qui est applicable lorsque le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

5. Sanctions et droit privé d'action

Article 150. Le Projet de loi 64 prévoit des sanctions administratives d'un montant maximal de 10 000 000 $ ou d'un montant correspondant à 2% du chiffre d'affaires mondial de l'exercice financier précédent de l'organisation, si ce dernier montant est plus élevé. Ces sanctions administratives s'appliquent dans le contexte d'une variété de

contraventions à la loi dont l'omission de déclarer un incident de confidentialité, le traitement de renseignements personnels en contravention avec la *Loi québécoise sur la protection des renseignements personnels dans le secteur privé*, de même qu'un manquement à l'obligation d'informer les individus d'un traitement automatisé.

Article 151. Le Projet de loi 64 prévoit un régime de sanctions selon lequel toute organisation qui :

- recueille, détient, communique à un tiers ou utilise un renseignement personnel en contravention de la Loi;
- omet de déclarer un incident de confidentialité;
- procède ou tente de procéder à l'identification d'une personne sans son autorisation alors que ses renseignements sont dépersonnalisés ou anonymisés;
- entrave le travail d'enquête de la Commission; ou
- contrevient à une ordonnance de la Commission

commet une infraction et est passible d'une amende de 15 000 $ à 25 000 000 $ ou à un montant correspondant à 4% du chiffre d'affaires mondial de l'organisation lors de l'exercice financier précédent si ce dernier montant est plus élevé.

Article 152. Le Projet de loi 64 prévoit un droit d'action personnel pouvant mener à l'octroi de dommages punitifs d'au moins 1 000 $ lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde. Le Projet de loi 64 ne prévoit aucune discrétion pour condamner le contrevenant à une somme moins élevée.

Commentaires

Les sanctions très sévères prévues par le Projet de loi 64 menacent l'investissement et l'innovation au Québec. De plus, un même incident de confidentialité ne devrait pas mener à de multiples sanctions de la part des régulateurs canadiens ou étrangers. Une même organisation pourrait ainsi se voir imposer plusieurs sanctions allant jusqu'à 4% de son chiffre d'affaires mondial chacune, et ce, pour un même événement. Cela augmente le risque que des sanctions déjà excessivement sévères puissent entrainer un effet multiplicateur avec des conséquences dévastatrices. Les principes fondamentaux d'équité doivent être considérés par le Projet de loi 64 afin que les organisations ne soient pas exposées à des enquêtes à la chaîne, provenant de plusieurs provinces ou de plusieurs pays, disposant chacun du pouvoir d'imposer d'importantes sanctions. Confirmer expressément que les organisations de juridiction fédérale sont soumises uniquement à la loi fédérale contribuera notamment à préserver ces principes fondamentaux d'équité.

Contrairement à la *Loi canadienne anti-pourriel*,[30] le Projet de loi 64 ne prévoit aucune disposition visant à protéger les organisations contre l'application simultanée des régimes de sanctions pénales et de droit d'action privée.

Le Projet de loi 64 n'accorde aucune discrétion permettant d'imposer une sanction moins élevée lorsqu'une violation entraine peu ou pas de préjudice, ou lorsque le nombre de

personnes affectées est élevé. Puisque les manquements aux obligations relatives à la protection de la vie privée concernent souvent un grand nombre d'individus, sans qu'un préjudice réel ou des dommages ne soient établis, le montant de 1 000 $ minimum par personne pourrait entrainer un effet multiplicateur et engendrer une sanction hors de proportion par rapport au préjudice subi.

La possibilité de se voir imposer des sanctions de cette envergure aurait un impact négatif sur l'évaluation des risques effectuée par les entreprises qui envisagent un investissement au Québec.[31] Les sanctions du RGPD offrent un exemple réel de cette possibilité. En effet, des études économiques ont établi un lien entre une baisse de 17.6% dans la fréquence des transactions et une baisse de 39.6% dans la valeur des transactions au sein de l'UE en comparaison avec les États-Unis à la suite de la mise en œuvre du RGPD. D'autres études ont également démontré un déclin marqué dans les investissements étrangers, avec une diminution de 22.2% dans le nombre de transactions mensuelles et une diminution de presque 42% dans la valeur des transactions par rapport aux entreprises américaines après la mise en place du RGPD. [32] Cette tendance a touché de manière disproportionnée les entreprises en nouvelles technologies dans leur processus de transition des anges financiers vers des investisseurs de capital de risque.[33]

Ces constats suggèrent qu'un régime de sanctions trop sévères aura un effet négatif direct sur les efforts du Québec pour promouvoir une économie fondée sur l'innovation[34] et pourrait forcer certaines compagnies à ne plus offrir aux résidents du Québec certains services innovants qui sont présentement disponibles ailleurs.

Recommandation #10 : Prévoir une certaine forme de coordination multi juridictionnelle des sanctions par les régulateurs, afin d'éviter qu'une organisation soit sanctionnée de manière disproportionnée ou à de multiples reprises en lien avec le même incident. Ce cadre devrait inclure un montant d'amendes globales maximum.

Recommandation #11 : Adopter un mécanisme similaire à celui prévu à l'art. 48 CASL afin d'éviter l'imposition d'amendes parallèles contre les organisations.

Recommandation #12 : Prévoir un pouvoir discrétionnaire d'octroyer des dommages moins élevés (tel que prévu à l'art. 38.1(3) de la Loi sur le droit d'auteur[35]) pour les cas où, si le montant minimal établi était accordé, « le montant total de ces dommages-intérêts serait extrêmement disproportionné à la violation » .

6. Droit de se retirer du profilage (*opt-out*) et traitement automatisé

Article 99. Le Projet de loi 64 prévoit qu'une organisation qui recueille des renseignements personnels en ayant recours à une technologie comprenant des fonctions permettant d'identifier une personne, de localiser ou d'effectuer un profilage doit, au

préalable, informer cette personne de l'utilisation de telles technologies ainsi que des moyens offerts, si disponibles, pour désactiver ces technologies. Le profilage est défini de la façon suivante : « la collecte et l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement ».

Article 102. Le Projet de loi 64 stipule qu'une organisation qui utilise des renseignements personnels dans un processus décisionnel exclusivement fondé sur un traitement automatisé de l'information doit, lors ou préalablement à la décision, en informer la personne concernée. Sur demande, l'organisation doit également dévoiler à la personne quels renseignements personnels ont été utilisés pour rendre cette décision, les motifs ainsi que les facteurs qui ont mené à ce résultat, en plus de l'informer de son droit de retirer son consentement. L'organisation doit de plus permettre à la personne de soumettre ses observations pour la révision de la décision.

Commentaires

Le Projet de loi 64 permet aux organisations d'utiliser des renseignements personnels sans obtenir de consentement pour des études et des analyses internes, pourvu que cet usage soit nécessaire pour ces études internes ou pour produire des statistiques et pourvu que l'information soit dépersonnalisée. Les BISi accueillent très positivement cette proposition qui apporte des bénéfices tant pour les consommateurs que les entreprises.

Toutefois, le Projet de loi 64 prévoit une définition trop large du profilage. La définition semble bien adaptée en ce qui concerne le profilage en ligne pour des objectifs publicitaires par des annonceurs tiers parties. Cette définition pourrait toutefois également s'appliquer par inadvertance à des objectifs d'affaires raisonnables tels que : les analyses internes menées par une organisation et visant ses clients dans le but d'améliorer le service offert; la gestion du risque de manière générale; la prévention de la fraude; la conformité ou la lutte contre le blanchiment d'argent. Chacun de ces objectifs d'affaires permet de fournir d'importants bénéfices aux consommateurs, mais exige la constitution de bases de données représentatives afin d'être efficace. Le retrait des renseignements personnels de certains individus de ces bases de données en raison de l'exercice d'un droit de retrait pourrait affecter négativement ou biaiser ces analyses.

Les dispositions du Projet de loi 64 concernant le traitement automatisé sont plus étendues que les dispositions équivalentes qui sont proposées par la LPRDE (ou prévues dans le RGPD). Celles-ci ne s'appliquent que lorsque la décision automatisée a un impact élevé. De façon similaire, l'exigence de transparence proposée par l'ISDE dans le cadre des réformes de la LPRDE favorise une approche équilibrée en mettant en lumière ces décisions automatisées tout en assurant la protection continue des informations commerciales confidentielles.[36] L'exigence liée au traitement automatisé dans le Projet de loi 64 manque de clarté et pourrait entrainer la divulgation d'informations confidentielles ou commercialement sensibles à propos des stratégies d'affaires, des opérations, ou des technologies de l'entreprise (incluant les algorithmes liés au traitement automatisé). De plus, même s'il est possible et approprié, dans certaines circonstances, de fournir aux individus des informations générales à propos de tels processus, l'ubiquité et la complexité de ce genre d'analyses rendraient impossible de fournir des informations spécifiques au sujet de toutes les étapes du processus technique menant ultimement à la

décision automatisée. Ces détails techniques ont peu de chance d'être utiles pour le consommateur moyen.

> **Recommandation #13 :** s'assurer que les lois québécoises de protection de la vie privée concernant le droit de retrait (*opt-out*) du profilage et du traitement automatisé comprennent des définitions précises et des exemptions pour faire en sorte qu'elles n'affectent pas par inadvertance ou n'interdisent pas des activités bénéfiques et qu'elles n'obligent pas la divulgation d'informations commerciales confidentielles.

7. Reprise des imperfections du RGPD

Commentaires

À haut niveau, le Projet de loi 64 a pour objectif de faire évoluer la loi québécoise en vue d'atteindre le statut approprié en vertu du RGPD et de générer des bénéfices pour les consommateurs et les entreprises québécoises.

Évidemment, le RGPD est unique et il est le reflet des spécificités propres à l'environnement européen, avec ses concepts distincts et des fondements juridiques extrêmement variés. Ainsi, le RGPD ne saurait être transposé tel quel dans l'environnement québécois et canadien. Bien que de nombreux enseignements puissent être tirés de l'approche de l'UE en matière de protection de la vie privée, il convient de prendre le temps nécessaire pour effectuer une réflexion approfondie afin de déterminer la meilleure façon d'incorporer les enseignements qui ont fait leurs preuves et démontré avoir apporté des bénéfices pour les consommateurs et les entreprises. Ceci étant, il est généralement reconnu que le RGPD souffre de sérieuses imperfections que le Québec devrait éviter d'importer dans son environnement.

Dans sa mouture actuelle, il appert que le Projet de loi 64 n'a pas pris en considération le nombre croissant d'éléments qui tendent à démontrer que le RGPD n'a pas toujours produit les résultats qu'il visait initialement, et a certainement entrainé des conséquences sérieuses et nombreuses qui n'étaient pas anticipées, incluant en :

- n'améliorant pas la confiance chez les utilisateurs;
- ayant un impact négatif sur l'accès en ligne des consommateurs;
- étant trop complexe à comprendre pour les consommateurs;
- ayant un impact négatif sur l'économie et les entreprises de l'UE;
- grugeant les ressources des entreprises;
- en ayant un impact négatif sur les entreprises européennes en démarrage;
- réduisant la compétition dans le domaine de la publicité numérique;

- étant trop complexe à mettre en œuvre pour les entreprises;
- n'étant pas interprété et mis en œuvre de manière cohérente par tous les États membres; et
- mettant à rude épreuve les ressources des régulateurs.[37]

D'un point de vue général, le Projet de loi 64 doit être conçu pour éviter ces effets non anticipés et indésirables, tout en incorporant les éléments du RGPD qui se sont avérés bénéfiques, lesquels sont essentiels pour l'obtention du statut d'adéquation par le Québec en vertu du RGPD.

> **Recommandation #14 :** S'assurer que le Projet de loi 64 évite les conséquences non anticipées et indésirables qui sont survenues lors de la mise en œuvre du RGPD, tout en établissant les bases pour l'obtention du statut d'adéquation pour faciliter les flux de données entre l'UE et le Québec.

8. Juridiction

Commentaires

En tant qu'entités dont les activités relèvent de la compétence fédérale, les BISi sont assujetties à la LPRDE depuis son entrée en vigueur en 2001.

Le Projet de loi 64 contient des exigences normatives qui sont significativement différentes des exigences et amendes actuellement prévues à la LPRDE. Ceci pourrait entrainer des conséquences négatives importantes, incluant : (i) un traitement injuste des BISi sous juridiction fédérale assujetties à de lourdes amendes, soulevant également des enjeux de double incrimination; (ii) une atteinte préjudiciable aux objectifs de protection de la vie privée et de support à l'innovation; et (iii) des conséquences indésirables pour les consommateurs.

Les BISi sont heureuses de prendre part au présent processus de consultation autant parce que nous possédons des filiales qui sont assujetties aux lois provinciales qu'en raison de notre intérêt marqué dans la promotion des intérêts de nos clients particuliers et entreprises dans la province. Toutefois, une telle participation ne doit pas être interprétée comme un assentiment quant à l'étendue de l'autorité règlementaire de la CAI sur les entreprises de compétence fédérale et quant à l'application du Projet de loi 64 aux entreprises fédérales.

Recommandation #15 : Clarifier que le Projet de loi 64 ne s'applique pas aux entreprises fédérales qui sont gouvernées par la LPRDE afin d'éviter entre autres des redondances règlementaires, le potentiel de doubles incriminations ainsi que les débats constitutionnels.

9. Courte période de mise en œuvre

Article 165. La majorité des dispositions du Projet de loi 64 doivent entrer en vigueur un an après avoir reçu la sanction royale, sous réserve de certaines exceptions.

Commentaires

Préoccupations : Un délai d'un an ne constitue pas une période suffisante pour permettre aux organisations de mettre en œuvre les changements importants que prévoit le Projet de loi 64. Les entreprises ont besoin de temps pour s'ajuster.[38]

Recommandation #16 : Accorder une période minimale de deux ans pour la mise en œuvre.

Recommandation #17 : S'assurer que les règlements et directives sont publiés préalablement à l'entrée en vigueur du Projet de loi 64.

10. Des exigences de sécurité mieux calibrées

Article 95. Le Projet de loi 64 prévoit que les organisations sont « responsable[s] de la protection des renseignements personnels » qu'elles détiennent et qu'elles doivent établir et mettre en œuvre des politiques de gouvernance et des pratiques qui « encadrent » la protection de ces renseignements.

Commentaires

Les standards de sécurité prévus par le Projet de loi 64 sont incompatibles avec les exigences établies à l'article 10 de la Loi sur le secteur privé, qui prévoit que les organisations doivent mettre en œuvre des mesures de sécurité qui sont « raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support ».

L'article 95 ne précise pas de seuil minimal de risque, de niveaux de sensibilité des renseignements ou de critères contextuels qui devraient déclencher une évaluation des risques en lien avec la protection de la vie privée (ex : étude d'impact sur la vie privée) et requiert que chaque évaluation soit faite en consultant la personne responsable de la

protection des renseignements personnels. Cette exigence n'est pas réaliste et pourrait retarder le lancement de nouveaux produits et services pour les consommateurs.

> **Recommandation #18 :** S'assurer que les exigences de sécurité prévues dans le Projet de loi 64 sont cohérentes entre elles, proportionnelles au risque, et que celles-ci fassent référence aux standards généralement acceptés par l'industrie.

11. Droit à l'oubli

Article 111. Le Projet de loi 64, dans sa forme actuelle, exigerait des organisations qu'elles détruisent ou anonymisent les renseignements personnels lorsque l'objectif pour lequel ils avaient été recueillis ou utilisés est accompli.

Article 113. Le Projet de loi 64 offrirait également aux individus le droit d'exiger qu'une organisation cesse de diffuser leurs renseignements personnels ou que soit désindexé tout hyperlien rattaché à leur nom qui permet d'accéder à des renseignements par un moyen technologique, lorsque les conditions établies par la Loi sur la vie privée dans le secteur privé sont respectées.

Commentaires

En ce qui concerne l'obligation de détruire ou d'anonymiser, il n'existe en ce moment aucune norme reconnue pour l'anonymisation qui permettrait d'assurer « l'irréversibilité » (en fait, ce genre de normes risque d'évoluer au rythme des avancées technologiques).

En ce qui a trait au droit à l'oubli, l'évaluation de l'opportunité de la « diffusion » de renseignements personnels susceptible de causer un préjudice grave à une personne sera difficile à appliquer et risque d'entrainer une certaine incertitude juridique ainsi que des défis opérationnels importants et coûteux. Bien que les commentaires de la ministre responsable sur cet article semblent suggérer que l'intention du législateur est de l'appliquer uniquement aux moteurs de recherche et aux entités qui fournissent des hyperliens menant à du contenu préjudiciable,[39] ceci devrait être clarifié pour mieux refléter cette intention. De plus, nous recommandons d'évaluer la possibilité de mettre en place un système complet d'exceptions et de limitations semblable à ce qui est prévu à l'article 17 du RGPD[40] pour assurer que les organisations maintiennent la capacité de se conformer à leurs obligations en lien avec la protection des renseignements personnels pertinents.

De plus, le terme « diffusion » est nouveau et sa signification est incertaine. Le terme est suffisamment large pour affecter les organisations de multiples manières au-delà des moteurs de recherche et autres fournisseurs de recherche, qui sont les cibles évidentes du remède de désindexation.

> **Recommandation # 19 :** L'obligation d'anonymisation devrait être contextualisée et être proportionnelle au risque pour éviter des coûts de conformité disproportionnés et l'incertitude légale.

Recommandation # 20 : Clarifier que les obligations de désindexation s'appliquent uniquement aux moteurs de recherche.

Recommandation # 21 : Retirer l'obligation de « non-diffusion ».

12. Seuil de déclaration des incidents

Article 95 : Le Projet de loi 64 inclut un nouveau seuil de déclaration d'incidents de confidentialité, qui exige que les autorités québécoises en matière de protection de la vie privée soient informées lorsqu'un incident de confidentialité présente un risque sérieux de préjudice.

Commentaires

Il n'est pas clair si cette disposition comporte un critère juridique différent de celui du « risque réel de préjudice grave » prévu à la LPRDE et au PIPA albertain.[41] Davantage d'incidents pourraient être inclus sous ce seuil, advenant qu'il soit réellement différent. Cette possibilité est susceptible d'introduire des difficultés dans la déclaration des incidents pour des activités impliquant des entreprises assujetties à la compétence provinciale.

Recommandation #22 : Mettre en place un seuil de déclaration des incidents aligné et cohérent avec la LPRDE et le PIPA albertain.

Notes et références

[1] https://www.osfi-bsif.gc.ca/Fra/fi-if/in-ai/Pages/cbrsk.aspx
[2] https://www.osfi-bsif.gc.ca/Fra/Docs/b10.pdf
[3] https://www.osfi-bsif.gc.ca/Fra/wn-qn/Pages/tchrsk.aspx
[4] LPRDE, S.C. 2000, c. 5.
[5] BC PIPA, S.B.C. 2003, c. 63.
[6] Alberta PIPA, S.A. 2003, c. P-6.5.
[7] Voir Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019) (mettant de l'avant des propositions centrées sur l'accroissement de la responsabilité plutôt que sur l'imposition de restrictions aux mouvements transfrontaliers de données).
[8] Règlement (EU) 2016/679 (Règlement général sur la protection des données).
[9] Les activités des BISi relèvent uniquement de la compétence fédérale et en conséquence nous sommes assujetties à la LPRDE. Bien que les BISi relèvent du régime fédéral, chacune d'entre elles possède des filiales, telles des filiales d'investissement et d'assurance, qui sont assujetties aux lois provinciales, dont notamment la *Loi sur la protection des renseignements personnels dans le secteur privé*, ainsi qu'aux lois applicables au secteur privé en Alberta et en Colombie-Britannique. Les exigences « d'équivalence » du Projet de loi 64 ont été largement critiquées. Jennifer Stoddart (ancienne Commissaire à la protection de la vie privée du Canada), "Quebec Takes the Lead in Privacy Law but Overreaches", *Financial Post* (15 July 2020) (critiquant les exigences « d'équivalence » et insistant sur le fait « qu'elles vont être difficiles à implémenter et devraient être reconsidérées quand le Projet de loi 64 sera lu en comité » (notre traduction); ministre Sonia Lebel, "Mémoire re: Loi modernisant des dispositions législatives en matière de protection des renseignements personnels" (25 mai 2020), à la p 21 (critiquant l' exigence « d'équivalence » du Projet de loi 64 et soulignant qu'elle « soulève des difficultés d'application »); Fasken LLP, "Projet de loi n° 64 et la réforme des lois québécoises sur la protection des renseignements personnels" (17 août 2020) (notant que « [l]es nouvelles exigences [concernant les transferts de données à l'extérieur du Québec] donneront lieu à des complications qui risquent d'être sans fin »). Voir aussi Institute of International Finance, "Data Flows Across Borders: Overcoming Data Localization Restrictions" (mars 2019), à la p 1 (observant que les restrictions aux mouvements transnationaux de données peuvent avoir des effets négatifs sur le système financier, notamment en « accroissant la complexité pour les TI et les données, nuisant à la gestion des risques, les pratiques de cybersécurité et de lutte au blanchiment d'argent des institutions financières, ainsi qu'en réduisant l'accès aux services financiers et aux marchés dans certains pays » (notre traduction)).
[10] Nous vous référons à la note 9 quant à la juridiction fédérale à laquelle les BISi sont assujetties. Il existe des outils pour garantir une solide protection de la vie privée lors du transfert des données par-delà les frontières. Voir par exemple : Commissariat à la protection de la vie privée du Canada, LPRDE Rapport sur les conclusions #2020-001, « Une banque fait preuve de transparence et assure un niveau de protection comparable à celui exigé par la Loi à l'égard du transfert de renseignements personnels à un tiers » (4 août 2020) (adoptant un accord de sous-traitance par lequel une BISi avait sous-traité ses services de lutte à la fraude a une tierce partie en s'assurant de la présence de garde-fous grâce à des limites contractuelles et des mesures de surveillance).
[11] Institute of International Finance, "Data flows across borders overcoming data localization restrictions", Mars 2019,
[12] Nous vous référons à la note 9 quant à la juridiction fédérale à laquelle les BISi sont assujetties
[13] CPTPP.
[14] CUSMA.
[15] Sur le besoin que les exigences de consentement soient adaptées à une économie moderne, voir Eloïse Gratton, "Beyond Consent-Based Privacy Protection" (11 Juillet 2016); Fred H. Cate & Viktor Mayer-Schonberger, "Notice and Consent in a World of Big Data" (2013) 3:2 *International Data Privacy Law* 67, à la p 67 (concluant que « la surutilisation des notions de notification et de consentement présente de plus en plus de défis dans une ère de « données massives » » et que, lorsque plusieurs consentements sont requis à différents moments dans le temps « plusieurs… utilisations qui ont des bénéfices individuels et

sociaux importants pourraient être tout simplement devenir trop coûteuses pour être accomplies ») (notre traduction).

[16] Voir Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019).

[17] Voir Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019) (notant le besoin de « réduire le risque de « fatigue du consentement » en retirant le besoin de consentir à des utilisations que la plupart des individus considéreraient comme raisonnables et en se concentrant sur les risques plus graves ») (notre traduction).

[18] Nous vous référons à la note 9 quant à la juridiction fédérale à laquelle les BISi sont assujetties. Voir Eloïse Gratton, "Beyond Consent-Based Privacy Protection" (11 juillet 2016), à la p 7 (insistant qu'il « n'est pas raisonnable de s'attendre à ce que l'individu moyen dédie une grande partie de leur temps à analyser et fournir une réponse significative aux demandes de consentement ») (notre traduction).

[19] RGPD, Art. 6; Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019); voir aussi les soumissions Commissariat à la protection de la vie privée du Canada à propos du Projet de loi 64 qui insiste sur le fait : « la protection des renseignements personnels ne peut reposer que sur le consentement », « Il n'est tout simplement pas réaliste ou raisonnable de demander aux individus de consentir à toutes les utilisations possibles de leurs données dans une économie de l'information aussi complexe que celle d'aujourd'hui », et suggère que le Québec devrait s'inspirer des « autres modèles de protection des données personnelles, qui tiennent compte des limites du consentement et qui cherchent par d'autres moyens à réaliser à la fois l'atteinte de l'intérêt public et la protection de la vie privée ».

[20] Voir Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019) (notant l'importance d' « harmoniser les cadres de protection de la vie privée à l'échelle nationale et internationale. »)

[21] Chambre de commerce des États-Unis, "'A Patchwork Is Not Acceptable': Making the Case for a National Privacy Law" (29 Juillet 2019).

[22] Département de la justice de la Californie, Bureau du procureur général, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations" (Août 2019), à la p 11.

[23] Roslyn Layton & Silvia Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices" (2019).

[24] Chambre de commerce des États-Unis, "'A Patchwork Is Not Acceptable': Making the Case for a National Privacy Law" (29 Juillet 2019).

[25] Information Technology and Innovation Foundation, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law" (5 Août 2019). En particulier, l'ITIF note que des lois sur la vie privée trop exigeantes risquent d'imposer à la fois des coûts de conformité et des inefficacités dans le marché. Les coûts de conformité incluent, pour ne donner qu'un exemple, les coûts d'amortissement que les entreprises doivent assumer en lien avec les nouvelles règlementations. Les inefficacités de marché constituent également des coûts indirects qui affectent les organisations en limitant la productivité et la valeur économique, incluant parmi les entreprises innovantes. Par exemple, il a été clairement démontré que la capacité à efficacement analyser les données génère des bénéfices économiques, tandis que de mauvaises lois sur la protection de la vie privée entrainent une réduction de la valeur économique. Sur les coûts de conformité pour le RGPD, voir PricewaterhouseCoopers, "Corporate GDPR Preparations to Stretch Past May 2018" (rapportant que, dans un sondage mené en 2018 auprès d'entreprises américaines, britanniques et japonaises, 47% des répondants planifiaient dépenser plus de 1 million $ en rapport avec la surveillance et la conformité au RGPD, et 30% planifiaient de dépenser entre 500 000 $ et 1 million $).

[26] The National Security Institute, "Privacy Regulation and Unintended Consequences for Security" (2019), soutenant l'idée que les protections de cybersécurité peuvent être renforcées par la mise en place de garde-fous de sécurité et d'une approche équilibrée; Roslyn Layton & Silvia Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices" (2019).

[27] Sur la notion de "Privacy by Design", voir Ann Cavoukian (ancienne Information and Privacy Commissioner of Ontario), "The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices" (janvier 2011).

[28] Voir Eloïse Gratton, "Beyond Consent-Based Privacy Protection" (11 juillet 2016), aux pp 40-44, 46-47 (adoptant une approche fondée sur le risque en matière de protection de la vie privée); Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019) (notant que « l'approche fondée sur le risque » peut « répondre aux préoccupations liées à la protection des renseignements personnels et encourager l'innovation ».)

[29] RGPD, Art. 25.

[30] CASL, S.C. 2010, c. 23, s. 48. Voir aussi le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des Communes, *La loi canadienne anti-pourriel : des précisions s'imposent* (Décembre 2017), aux pp 17-20 (rapportant les préoccupations de témoins concernant les droits d'action privés dans la Loi).

[31] Voir Les Echos, « Le règlement européen sur les données effraie les entreprises » (Avril 2017) (rapportant que, dans un sondage mené en 2017 auprès de 900 larges entreprises au sujet des effets des pénalités prévues dans le RGPD (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire annuel de l'entreprise), environ un répondant sur cinq craignait devoir réduire le nombre de ses employés en cas d'amende, et un autre répondant sur cinq craignait de devoir fermer boutique entièrement.

[32] Jian Jia *et al.*, "The Short-Run Effects of GDPR on Technology Venture Investment" (National Bureau of Economic Research Working Paper, Novembre 2018) (pp. 4-5)); Jian Jia *et al.*, "GDPR and the Localness of Venture Investment" (2019) (concluant également que « l'implémention du RGPD en mai 2018 a des effets négatifs sur l'investissement en capital de risque dans l'UE et que les effets sont plus prononcés lorsque les entreprises et les investisseurs principaux ne sont pas dans le même pays ou union » (notre traduction); Michal S. Gal & Oshrit Aviv, "The Competitive Effects of the GDPR" (2020) 16:3 *Journal of Competition Law & Economics* 349, citant, *inter alia,* Merrill Corporation, GDPR Burdens Hinder M&A Transactions in the EMEA Region (13 novembre 2018) (58% des professionnels en fusions et acquisitions recensés ont mentionné avoir travaillé sur des transactions qui ont échouées en raison des préoccupations des parties concernant leur conformité aux règles du RGPD).

[33] Jian Jia *et al.*, "The Short-Run Effects of GDPR on Technology Venture Investment" (National Bureau of Economic Research Working Paper, Novembre 2018) (pp. 8, 19, 40-42, Tableaux 6-8).

[34] Voir Ministre Sonia LeBel, "Mémoire re: Loi modernisant des dispositions législatives en matière de protection des renseignements personnels" (25 mai 2020), aux pp, 4, 17 (notant que les objectifs des amendements législatifs sont de « soutenir l'innovation »).

[35] *Loi sur le droit d'auteur*, R.S.C. 1985, c. C-42.

[36] Innovation, Science et Développement Économique Canada, *Renforcer la protection de la vie privée dans l'ère numérique: Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques* (2019) (qui propose de « [f]ournir des mesures de contrôle plus efficaces et accroître la transparence pour les individus [en]… Exige[ant que les individus soient informés de l'utilisation de processus décisionnels automatisés, des facteurs ayant une incidence sur la décision et de sur quoi la décision a une incidence, ainsi que de la logique sur laquelle la décision est fondée. Une telle exigence ne s'étendrait pas à la communication de renseignements commerciaux confidentiels à un individu. »

[37] Voir, par exemple, Center for Data Innovation, "What the Evidence Shows About the Impact of the GDPR After One Year" (17 June 2019) (fournissant une liste de sources détaillant les « sérieuses et nombreuses » conséquences non souhaitées du RGPD); Jian Jia *et al.*, "The Short-Run Effects of GDPR on Technology Venture Investment" (National Bureau of Economic Research Working Paper, Novembre 2018) (concluant qu'il existe « un effet négatif différencié sur les entreprises européennes depuis de déploiement du RGPD en comparaison avec les entreprises américaines » et que « les effets négatifs du RGPD sur l'investissement dans les technologies semble être particulièrement marqué pour les entreprises naissantes, de 0 à 3 ans » avec des pertes d'emplois estimées « entre 3 604 et 29 819, soit 4.09 à 11.20% des emplois créés par les entreprises de 0 à 3 ans dans notre échantillon » (pp. 4-5) (notre traduction); Competitive Enterprise Institute, "European Union's General Data Protection Regulation and Lessons for U.S. Privacy Policy" (2018), à la p 1 (concluant que le RGPD « va significativement porter préjudice à la compétition et l'innovation non

seulement en Europe, mais partout dans le monde ») (notre traduction); Jian Jia *et al.*, "GDPR and the Localness of Venture Investment" (2019) (concluant également que « l'implémentation du RGPD en mai 2018 a des effets négatifs sur l'investissement en capital de risque dans l'UE et que les effets sont plus prononcés lorsque les entreprises et les investisseurs principaux ne sont pas dans le même pays ou union » (notre traduction); Roslyn Layton & Silvia Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices" (2019) (rapportant que « en conséquence du RGPD, les entreprises sont confrontées à de nombreux défis pour se conformer avec des règles coûteuses et complexes, des définitions larges de ce que sont les renseignements personnels identifiables, et des risques accrus d'amendes et/ou de poursuites pour des manquements à ces obligations, des vulnérabilités et des manques de conformité » et « des effets secondaires concernant la sécurité ont été remarqués ») (notre traduction); National Security Institute, "Privacy Regulation and Unintended Consequences for Security" (2019) (expliquant quelles conséquences non souhaitées les lois sur la vie privée peuvent avoir sur la sécurité); Michal S. Gal & Oshrit Aviv, "The Competitive Effects of the GDPR" (2020) 16:3 *Journal of Competition Law & Economics* 349 (concluant que « le coût de la protection des données dans le cadre du RGPD est plus élevé que ce qui était envisagé jusqu'ici » et que « le RGPD crée deux effets négatifs principaux sur la compétition et l'innovation : il limite la compétition sur les marchés de données, créant des structures de marchés plus concentrées et consolidant les pouvoirs de ceux qui sont des joueurs importants sur le marché; et il limite les échanges de données entre différents acteurs qui collectent des données, empêchant ainsi la réalisation de certaines synergies qui pourraient mener à de meilleurs connaissances fondées sur des données) (notre traduction); "GDPR – Challenges for Reconciling Legal Rules with Technical Reality" (2020 European Symposium on Research in Computer Security Conference Paper) (remarquant une divergence entre le RGPD et la réalité technologique); Heli Koski & Nelli Valmari, "Short-Term Impacts of the GDPR on Firm Performance" (2020) (qui a déterminé que « les coûts engendrés par le RGPD durant la première année de son implémentation étaient substantiels » et que « les PMEs avec des besoins élevés en termes de données furent les plus désavantagées ») (notre traduction).

[38] Voir PricewaterhouseCoopers, "Corporate GDPR Preparations to Stretch Past May 2018" (rapportant que, dans un sondage mené en 2018 auprès d'entreprises américaines, britanniques et japonaises, alors que le RGPD a été adopté en 2016 et devait entrer en vigueur en mai 2018, seulement 10% des répondants avaient terminé leurs préparations opérationnelles à la date de l'enquête).

[39] Ministre Sonia LeBel, "Mémoire re: Loi modernisant des dispositions législatives en matière de protection des renseignements personnels" (25 mai 2020), à la p 6.

[40] RGPD, Art. 17.

[41] LPRDE, S.C. 2000, c. 5, s. 10.1; Alberta PIPA, S.A. 2003, c. P-6.5, s. 34.1.