CI– 015M
C.P. – PL 64
Protection des renseignements personnels

Le 10 septembre 2020

L'Information Accountability Foundation (IAF) se saisit de l'occasion pour présenter ses réflexions sur le projet de loi relatif à la protection des renseignements personnels déposé par le gouvernement du Québec, en vue de son adoption à l'Assemblée nationale. L'IAF est une organisation internationale sans but lucratif qui poursuit deux objectifs, à savoir faire de la recherche sur la protection des données et de la vie privée dans une perspective de responsabilisation et organiser des activités de sensibilisation à cet égard. L'intégration du dialogue international sur la responsabilité (*Global Accountability Dialog*) a marqué la mise en pratique du principe de la responsabilité énoncé par l'Organisation de Coopération et de Développement Économiques (OCDE) dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* à appliquer dans une économie et une société numériques[1]. L'IAF a réalisé des projets de recherche en Europe, en Asie et en Amérique, dont trois au Canada. En 2014, elle a lancé à Montréal un dialogue sur l'utilisation des données par le gouvernement, en collaboration avec l'ancienne commissaire à la protection de la vie privée du Québec, Jennifer Stoddart[2]. La prochaine refonte des lois sur la protection de la vie privée est l'un des champs d'intérêt de l'IAF, et c'est dans cette perspective qu'elle énonce les commentaires présentés ci-dessous.

L'IAF est d'accord avec l'évaluation du gouvernement du Québec indiquant que le moment est venu de mettre à jour la loi en vigueur actuellement, qui a été promulguée il y a pratiquement trente ans. Au Canada, le Québec est l'une des premières provinces à avoir adopté une loi sur la protection des renseignements personnels dans le secteur privé, soit en 1993. La province a été une pionnière en la matière en raison du fait que la vie privée est et demeure un droit fondamental enchâssé dans sa *Charte des droits et libertés de la personne*. La plupart des droits fondamentaux demeurent assez simples à comprendre. Il en va différemment pour la protection de la vie privée. En fait, les chercheurs ont eu du mal à traduire l'essence même du concept de protection de la vie privée dans une définition. Donc, au lieu de tenter de définir le droit en tant que tel, il est souvent plus simple de décrire les intérêts que ce droit recouvre. Ces intérêts sont au nombre de trois, que voici :

- Le premier, c'est l'intérêt, chez l'être humain, pour l'intimité. Nous avons tous besoin de nous retrouver dans un endroit où personne ne peut nous observer ni faire intrusion dans notre vie privée. Cet intérêt est tributaire de la confidentialité de ce qui se passe dans un ménage, ainsi que dans les documents et les dossiers qui concernent ce ménage. À bien des égards, notre intérêt pour l'intimité se trouve contrarié par le terrain d'observation que la société moderne est devenue, où il est possible de créer un dossier sur le comportement sans les bons vieux dossiers papier[3].
- Le deuxième, c'est l'intérêt, chez les gens, de se définir eux-mêmes, et non d'être définis par les traces numériques qu'ils laissent derrière eux. Cet intérêt s'observe dans les mesures liées à

[1] https://www.oecd.org/fr/sti/ieconomie/privacy-guidelines.htm
[2] *Organizational Accountability, Government Use of Private Sector Data, National Security, and Individual Privacy*
[3] L'article 5 du chapitre I de la partie I de la *Charte des droits et libertés de la personne* du Québec stipule que : « Toute personne a droit au respect de sa vie privée. »

l'autonomie de la personne ou encore à sa capacité d'exercer un contrôle sur les données qui se rapportent à sa réputation[4].

- Le troisième, c'est l'intérêt, pour une personne, d'obtenir un traitement équitable. Il s'agit, pour cette personne, de se faire traiter équitablement, de ne pas être l'objet de discrimination, au moyen de décisions fondées sur des données exactes. Étant donné que les processus et les ordinateurs fonctionnent essentiellement à partir de données (p. ex., l'Internet des objets), les organismes responsables de la protection de la vie privée et les spécialistes en la matière s'occupent en grande partie dans leur travail d'assurer un traitement équitable[5].

L'interaction entre la technologie et ces trois intérêts aujourd'hui est très différente de ce qu'elle était il y a trente ans. La loi est antérieure à l'apparition de risques et d'avantages liés à l'arrivée d'Internet, des téléphones intelligents, des voitures connectées, de l'analytique avancée et de l'Internet des objets. Lorsqu'on envisage d'adopter une loi sur la protection des renseignements personnels, il faut tenir compte des liens entre cette protection et les autres droits fondamentaux et intérêts. Bien que le droit à la vie privée soit fondamental, ce n'est pas un droit absolu. Tout le monde a des droits et des intérêts autres, tout aussi importants. Il s'agit entre autres de l'intérêt pour l'amélioration de la santé et de l'éducation, du droit à être employé et à créer une entreprise. Il s'agit également du droit à l'information et de celui de prendre des décisions fondées sur des données validées. Il est parfois plus efficace de faire primer ces intérêts en les regroupant avec ceux d'autres personnes pour en faire des intérêts de société. Ainsi, bien que les gens se soucient de l'incidence de leur dossier médical sur leur réputation et leur condition sociale, ils ont avantage à consentir à ce que les données servent à la recherche sur les soins de santé tout en étant l'objet d'une protection adéquate. Tous les Québécois sont animés par ce souci de voir les soins de santé s'améliorer grâce à la recherche. Pour être excellente, une loi sur la protection des renseignements personnels relie un ou plusieurs de ses intérêts, ce qui permet de concilier, toutes proportions gardées, tous les droits et toutes les libertés.

Bien que selon l'IAF, le moment soit venu de légiférer, elle est d'avis que cette législation pourrait concilier davantage les intérêts de tous les Québécois. Il s'agit là de commentaires généraux, qui indiquent que la loi qui est proposée devrait comporter des dispositions qui font évoluer la société en la dynamisant. Notamment, le projet de loi devrait être structuré de façon à tenir compte de toute la gamme des droits et des intérêts en fonction des recours de manière à ce qu'ils soient reliés, toutes proportions gardées, à l'intimité, à l'autonomie, au traitement équitable et à d'autres droits et intérêts. La proportionnalité est généralement présentée comme une exigence administrative pour le gouvernement, qui doit faire un compromis entre les droits fondamentaux des gens et le pouvoir de l'État, utilisateur de données sur ces gens. La proportionnalité est différente lorsqu'elle est présentée comme une exigence du secteur privé. Elle se rapporte aux utilisateurs avertis de données soucieux de concilier toute la gamme des intérêts de tous les intervenants. Bien qu'on mette l'accent sur la multitude d'intérêts des gens à qui les données se rapportent, l'utilisateur de données responsable sait

[4] L'article 4 du chapitre I de la partie I de la *Charte des droits et libertés de la personne* du Québec stipule que : « Toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation. »

[5] L'article 10 du chapitre I.1 de la partie I de la *Charte des droits et libertés de la personne* du Québec prévoit ce qui suit : « 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, l'orientation sexuelle, l'état civil, l'âge sauf dans la mesure prévue par la loi, 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. »

également tenir compte des intérêts des autres intervenants, qui risquent de subir les conséquences du traitement, ou de l'absence de traitement des données.

Une définition du principe de la responsabilité en pensant à l'avenir

Le projet de loi introduit le concept de responsabilité et établit très précisément la façon d'être responsable en énonçant certaines obligations particulières. Cependant, il n'en définit ni l'objet ni la véritable fonction. Le point de départ, c'est le principe général selon lequel les organisations devraient traiter de façon responsable les données et qu'elles devraient être imputables du traitement responsable qu'elles en feront.

Quant à l'objectif général lié à la responsabilité, il est absent du projet de loi. Ses dispositions sont à la fois incomplètes et trop précises pour un projet de loi censé renouveler le cadre qui s'applique à la protection des renseignements personnels. En 2009, les éléments essentiels du principe de la responsabilité ont été adoptés à l'issue d'un dialogue mondial[6] et ils jettent les bases de la façon dont ce principe de la responsabilité qui s'inscrit dans un programme élaboré de gestion de la vie privée est décrit au Canada[7]. Ce projet de loi est loin d'être à la hauteur de ces éléments essentiels comme c'est démontré dans le tableau ci-dessous, loin de les moderniser pour les décennies à venir.

Éléments essentiels du principe de la responsabilité en 2009	Projet de loi du Québec
Engagement des organisations envers le principe de la responsabilité et adoption de politiques internes conformes aux critères externes	C'est le plus haut dirigeant de l'entreprise qui est chargé d'assurer la protection des renseignements personnels. Le titre et les coordonnées de la personne responsable doivent être publiés. Il faut que cette personne établisse les politiques et les pratiques en matière de gouvernance destinées à assurer la protection des renseignements personnels (la conservation et la destruction des renseignements, les rôles et les responsabilités, les procédures à suivre pour le traitement des plaintes), proportionnellement à la nature et à la portée des activités, les approuve, les mette en œuvre et les publie sur le site Web de l'entreprise.

[6] Un représentant du Commissariat à la protection de la vie privée du Canada a aidé à définir les éléments essentiels du principe de la responsabilité.

[7] *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/gl_acc_201204/

Mécanismes destinés à mettre en œuvre les politiques sur la protection de la vie privée, notamment les outils, la formation et les programmes de sensibilisation	Il faut procéder à l'évaluation des facteurs liés à la protection des renseignements personnels des systèmes d'information et des projets liés à la prestation de services électroniques. Il faut consulter la personne responsable dès le début du projet. Dans le projet, il faut autoriser la communication des renseignements personnels informatisés dans un format couramment utilisé. La personne responsable peut proposer des mesures liées à la protection des renseignements personnels à appliquer au projet : - la nomination d'une personne responsable de la mise en œuvre des mesures liées à la protection des renseignements personnels; - des mesures liées à la protection des renseignements personnels dans tout document concernant le projet; - la description des responsabilités concernant la protection des renseignements personnels, dont devront s'acquitter les participants au projet; - les activités de formation sur la protection des renseignements personnels, à l'intention des participants au projet.
Systèmes de surveillance interne continue et de vérification externe	
Transparence et mécanismes de participation individuelle	Il faut que cette personne établisse les politiques et les pratiques en matière de gouvernance destinées à assurer la protection des renseignements personnels (la conservation et la destruction des renseignements, les rôles et les responsabilités, les procédures à suivre pour le traitement des plaintes), proportionnellement à la nature et à la portée des activités, les approuve, les mette en œuvre et les publie sur le site Web de l'entreprise.
Mesures correctives et moyens visant à appliquer la loi à l'extérieur	
	S'il y a des motifs de croire qu'un incident lié à la confidentialité de renseignements personnels s'est produit, il faut prendre des mesures raisonnables en vue de réduire le risque de

	préjudice et d'empêcher que ce genre d'incident se reproduise. - Si l'incident comporte un risque de préjudice grave, voici ceux qui doivent en être avisés : – la Commission d'accès à l'information du Québec (CAI); – la personne dont les renseignements personnels sont concernés. - Toute personne ou tout organisme qui pourrait réduire le risque peuvent également être avisés. - Il faut tenir compte des éléments ci-dessous en évaluant le risque de préjudice : – la nature délicate des renseignements concernés; – les conséquences anticipées de leur utilisation; – la probabilité que ces renseignements soient utilisés à des fins préjudiciables. - Il faut tenir un registre des incidents de confidentialité. Voici la définition du terme « incident d'atteinte à la confidentialité » : - accès non autorisé par la loi à des renseignements personnels; - utilisation non autorisée par la loi de renseignements personnels; - communication non autorisée par la loi de renseignements personnels; - disparition de renseignements personnels ou tout autre atteinte à la protection de ce genre de renseignements.

Comme l'illustre le tableau ci-dessus, le projet de loi fait abstraction de certains éléments essentiels du principe de la responsabilité de 2009, il omet de les moderniser, et pour le secteur privé, reprend, dans une certaine mesure, les modifications apportées à la *Loi sur la protection des renseignements personnels numériques* pour les ajouter à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[8], qui a introduit l'obligation de signaler les atteintes à la protection des données.

Un renouvellement du principe de la responsabilité pour l'avenir numérique du Québec

[8] https://laws-lois.justice.gc.ca/fra/LoisAnnuelles/2015_32/

La stratégie numérique du Canada a fait ressortir le fait que les données sont le moteur des économies au pays. Celle-ci vise à permettre aux Canadiens de profiter des possibilités offertes par l'économie numérique tout en les tenant à l'abri des menaces que comporte l'adoption des technologies numériques, notamment les menaces pour la sécurité des renseignements personnels et pour la protection de la vie privée[9]. Pour que les Québécois puissent profiter de l'ère actuelle, axée sur l'utilisation des données, le Québec a besoin d'un cadre de responsabilisation qui tient compte des avantages et des inconvénients des technologies numériques et les anticipe, en particulier les technologies qui ne nécessitent aucune intervention humaine. Ce cadre, connu sous le nom de Responsabilité démontrable liée au traitement équitable (*Fair Processing Demonstrable Accountability*), comprend, entre autres exigences, un processus d'évaluation qui concilie le risque de préjudice et les avantages pour les gens, que représentent les technologies numériques. Celles-ci sont des outils, des systèmes, des appareils et des ressources électroniques qui servent à générer des données, à les stocker et à les traiter[10]. Dans ses travaux au Canada et dans d'autres territoires de compétence, l'IAF se penche sur la façon dont les éléments essentiels du principe de la responsabilité pourraient être mis à jour compte tenu du monde très connecté dans lequel nous vivons aujourd'hui. Ces travaux ont été présentés dans le projet d'administration améliorée des données, le projet sur les évaluations de l'incidence des données sur l'éthique ou *Ethical Data Impact Assessments* (EDIA) en collaboration avec le commissaire à la protection de la vie privée de Hong Kong[11]. L'IAF publiera d'autres éléments mis à jour pour tenir compte des éléments du cadre de responsabilité démontrable liée au traitement équitable plus tard en 2020. En voici cependant un résumé ci-dessous. Bref, les dispositions liées au principe de la responsabilité dans le projet de loi sont loin des exigences énoncées dans le cadre de responsabilité démontrable liée au traitement équitable. Ces dispositions ne sont pas suffisamment détaillées pour tenir compte des progrès technologiques ainsi que de la surveillance et des mesures correctives nécessaires pour que le principe de la responsabilité soit fiable et qu'il donne les résultats escomptés. Ces dispositions présentent une vision étroite de la portée de la responsabilité.

À titre d'exemple, voici ce que devraient exiger les éléments liés au principe de la responsabilité démontrable à l'ère numérique :

- L'engagement de l'organisation à l'égard du principe de la responsabilité démontrable liée au traitement équitable et l'adoption de politiques internes conformes aux critères externes et aux principes établis en matière de traitement équitable – Par souci d'engagement, les organisations devraient définir les valeurs et les principes liés au traitement équitable, qui se traduisent ensuite en politiques et en processus organisationnels. Ces principes devraient découler de l'organisation et s'ajouter aux lois et aux règlements. Ils peuvent aller plus loin que les exigences énoncées dans la loi, mais ils devraient s'harmoniser avec la législation, la réglementation et les codes de conduite officiels en vigueur.
- Des mécanismes visant à mettre en œuvre des politiques sur le traitement équitable, notamment des évaluations des effets défavorables en fonction des risques, des outils, ainsi que des programmes de formation et de sensibilisation – Il faudrait procéder à des évaluations de l'incidence sur le traitement équitable dans les cas où l'analyse avancée des données peut avoir des répercussions importantes sur les gens ou lorsque des décisions axées sur les données sont

[9] *La Charte numérique du Canada en action : un plan par des Canadiens, pour les Canadiens*, https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00109.html

[10] Department of Education and Training, gouvernement de l'État de Victoria, Australie 2019

[11] https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Hong-Kong-Report-FINAL-for-electronic-distribution-10.22.18.pdf; https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf

prises sans l'intervention d'autres personnes. Lorsqu'une utilisation fondée sur des données analytiques risque d'avoir une incidence sur des gens ou à un niveau plus élevé (p. ex., groupes de personnes et société), les avantages et les effets défavorables devraient être définis explicitement. Les effets défavorables devraient ensuite être atténués dans la mesure du possible. Les organisations devraient utiliser un processus de « traitement équitable dès la conception » afin d'intégrer leurs principes liés au traitement équitable et les exigences des politiques dans leur processus de conception de systèmes de technologie numérique afin que la société, les groupes de gens ou les personnes elles-mêmes, et pas seulement les organisations, gagnent en valeur grâce aux activités liées au traitement des données.

- Processus d'examen interne qui évaluent l'incidence sur le traitement équitable lorsque le risque est plus élevé ainsi que l'ensemble du programme lié au traitement équitable – Les initiatives liées aux données présentant un risque plus élevé, ayant une incidence plus importante ou entraînant des effets défavorables qui n'ont pas été suffisamment pris en compte, devraient être renvoyées à des groupes de décideurs dans l'organisation à un plus haut niveau aux fins d'examen et d'approbation. Le processus de transmission à un niveau supérieur doit être fondé sur l'approche de gestion des risques externes qui sont hors du contrôle du programme et en faire partie, et il devrait tenir compte du fait que les problèmes soulevés dans le cadre de l'évaluation de l'incidence sur le traitement équitable ont été résolus et que les activités avancées de traitement des données ont été menées comme prévu.
- Transparence des gens et des organisations et mécanismes de participation individuelle – Les principes liés au traitement équitable qui régissent les activités avancées relatives au traitement des données et qui sous-tendent les décisions devraient être largement diffusés, et les processus devraient être transparents dès le départ dans la mesure du possible. En outre, toutes les préoccupations des gens et de la société devraient être prises en compte et documentées dans le cadre du processus d'évaluation de l'incidence sur le traitement équitable, et des mécanismes de rétroaction liés à la responsabilité devraient être établis.
- Mesures correctives et moyens visant à appliquer la loi à l'extérieur – Les organisations devraient être prêtes à démontrer aux organismes de réglementation ayant autorité, notamment les organismes de certification auxquels elles sont assujetties, le bien-fondé des processus internes, la pertinence des activités avancées liées au traitement des données, et les situations dans lesquelles le traitement des données a ou peut avoir une incidence importante sur les gens.

À défaut de traiter l'un ou l'autre de ces éléments liés à la responsabilité démontrable à l'égard des technologies numériques, le projet de loi sera désuet avant même d'être adopté. Il demande aux secteurs public et privé d'utiliser des ressources limitées pour mettre en place des processus incapables de relever les défis numériques d'aujourd'hui et de demain.

La légitimité d'une collecte de renseignements personnels ne devrait pas reposer uniquement sur le consentement

Dans le *Rapport sur le consentement* de 2016-2017 du Commissariat à la protection de la vie privée, il a été reconnu que le consentement peut ne pas convenir dans certaines circonstances, p. ex., lorsque les consommateurs n'ont pas de relation avec l'organisation qui utilise leurs données et lorsque l'usage qui sera fait des renseignements personnels n'est pas connu au moment de la collecte, ou qu'il est trop complexe pour être expliqué aux gens. Le consentement est un élément fondamental de la LPRPDE. Légalement, les organisations doivent obtenir un consentement valable avant de recueillir, d'utiliser et de divulguer les renseignements personnels d'une personne, sous réserve de certaines exceptions.

Lorsque la LPRPDE a été adoptée, les interactions avec les entreprises étaient généralement prévisibles, transparentes et bidirectionnelles. Les gens comprenaient pourquoi l'entreprise avec laquelle ils faisaient affaire avait besoin de certains renseignements personnels. Les moments où la collecte de renseignements avait lieu étaient clairement fixés, et les personnes concernées avaient donné leur consentement. Mais il est de plus en plus difficile d'obtenir le consentement des gens, et celui-ci ne parvient pas à les protéger dans l'environnement numérique. Bien que le consentement continue de jouer un rôle décisif dans la protection du droit à la vie privée lorsqu'il peut être accordé en connaissance de cause, les flux d'information complexes et les processus opérationnels impliquant une multitude de tiers intermédiaires, tels que les moteurs de recherche, les plateformes et les agences de publicité, ont ébranlé le modèle de consentement. À l'ère des mégadonnées, de l'Internet des objets, de l'intelligence artificielle et de la robotique, les consommateurs ne savent plus vraiment qui traite leurs données et à quelles fins. Pour les particuliers, l'utilisation des services numériques modernes a un coût : ils doivent accepter, dans une certaine mesure, que les entreprises doivent inévitablement recueillir et utiliser leurs renseignements personnels en échange d'un produit ou d'un service[12]. Étant donné que, on le sait maintenant, les relations d'affaires ne sont plus bidirectionnelles et qu'il n'est pas toujours possible d'obtenir un consentement, ça ne sert à rien de rédiger un projet de loi, censé moderniser la loi, qui impose le consentement comme condition à remplir pour la collecte de renseignements personnels.

En soutenant que des renseignements personnels peuvent également être recueillis auprès d'un tiers s'il y a une raison sérieuse et légitime, on se trompe parce que l'une ou l'autre des conditions suivantes doit être remplie : (1) les renseignements sont recueillis dans l'intérêt de la personne concernée et ne peuvent être recueillis auprès d'elle en temps opportun, ou (2) il faut les recueillir auprès d'un tiers afin d'en assurer l'exactitude. Autrement dit, il n'y a que deux raisons valables. Cette disposition est beaucoup trop contraignante pour être utile et légitime.

Étant donné que le projet de loi tente, semble-t-il, d'intégrer de nombreux éléments du *Règlement général sur la protection des données* de l'Union européenne (RGPD), il vaudrait mieux intégrer également la licéité du traitement des données énoncée à l'article 6 du règlement. Cet article contient six moyens juridiques de traiter les données, dont les intérêts légitimes. Le concept d'intérêt légitime dans le RGPD est beaucoup plus vaste que la raison légitime dans le projet de loi. Il s'agit du traitement « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant[13]. » Dans les paragraphes qui en constituent le préambule, le RGPD stipule que le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné, le traitement de données à caractère personnel à des fins de marketing direct peut être considéré comme étant réalisé pour répondre à un intérêt légitime, lorsque les responsables du traitement qui font partie d'un groupe d'entreprises ou d'établissements affiliés à un organisme central peuvent avoir un intérêt légitime à transmettre des données à caractère personnel au sein du groupe d'entreprises à des fins administratives internes, y compris le traitement de données à caractère personnel relatives à des clients ou à des employés[14]. Il en ressort clairement que les traitements décrits dans ces paragraphes

[12] *Rapport sur le consentement* de 2016-2017, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201617/ar_201617/

[13] Article 6(e) du RGPD

[14] Paragraphes 47 et 48 du RGPD

sont des exemples et que d'autres circonstances qui satisfont aux exigences du RGPD sont autorisées, c'est-à-dire celles nécessaires aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par le tiers, ET celles sur lesquelles les intérêts ou les droits et libertés fondamentaux de la personne concernée n'ont pas préséance[15]. La façon dont les intérêts légitimes sont abordés dans le RGPD démontre à quel point la raison légitime est étroite, inapplicable et dépassée dans le projet de loi du Québec.

L'équivalence des protections juridiques n'est pas la bonne structure pour les transferts de renseignements personnels

Le projet de loi prévoit qu'avant de communiquer des renseignements personnels à l'extérieur du Québec, il faut procéder à une évaluation des facteurs liés à la vie privée en tenant compte de ce qui suit :

1. la sensibilité des renseignements;
2. la finalité de leur utilisation;
3. les mesures de protection qui s'y appliqueraient;
4. le cadre juridique applicable dans l'État dans lequel les renseignements seraient communiqués, notamment le degré d'équivalence du cadre juridique avec les principes liés à la protection des renseignements personnels applicables au Québec.

L'information peut être communiquée si l'évaluation démontre que celle-ci bénéficierait d'une protection équivalant à celle prévue à la présente loi[16]. À défaut de respecter cette norme, aucun transfert n'est autorisé. Un tel mécanisme de transfert limité n'est pas économiquement viable, est néfaste pour les entreprises situées au Québec et pour l'économie du Québec en général, est isolationniste, et n'est pas le genre de modernisation visée par le présent projet de loi.

Le projet de loi a pour but de réglementer la communication de renseignements personnels au Québec dans les secteurs privé et public, ainsi que celle des renseignements personnels qui proviennent du Québec, mais qui pourraient être communiqués dans un autre territoire de compétence. La première loi sur la protection de la vie privée a démontré qu'il était difficile de départager les champs de compétence dans l'espace et le temps. Le Canada a décidé que la protection de la vie privée était du ressort fédéral, les responsabilités de surveillance et d'application de la loi étant réparties entre le gouvernement fédéral et les provinces. Tout comme en Europe, cette approche signifie que tous les territoires de compétence qui font partie du système sont réputés avoir les capacités nécessaires pour remplir leur rôle respectif. Le projet de loi, qui a entre autres l'obligation d'assurer des protections équivalentes dans d'autres territoires de compétence, ne précise pas clairement que les autres territoires de compétence au Canada, en raison de leur appartenance à ce système fédéral, ont les capacités nécessaires et qu'ils sont donc équivalents. Si ce n'est pas le cas, cette situation a des répercussions pratiques sur le fonctionnement des entreprises. Par exemple, il serait malheureux qu'un superviseur n'ait pas accès aux données nécessaires pour encadrer un employé au Québec parce que la province au Canada, dont il est originaire, a une loi qui atteint des objectifs semblables, mais qui n'est pas équivalente sur le plan de la structure.

[15] Paragraphe 47 du RGPD
[16] Article 17

On pourrait dire la même chose des transferts au-delà du Québec. Beaucoup de Québécois font des affaires à l'étranger. Bon nombre sont employés par des entreprises aux États-Unis, par exemple. En 2019, 71,2 % des données exportées en provenance du Québec ont été transférées aux États-Unis[17]. L'équivalence (désignée sous le nom d'adéquation, mais au sens d'équivalence) pour les transferts a été intégrée dans la loi européenne sur la protection de la vie privée dans le secteur privé, le RGPD. Cependant, l'Europe n'a réussi à trouver qu'une poignée de territoires de compétence adéquats, et tous doivent faire l'objet d'un examen par la Commission européenne. Heureusement, le RGPD permet des dérogations lorsqu'une entreprise peut garantir que les données européennes seront protégées par les responsables du traitement des données selon les normes européennes. Toutefois, même ces dérogations ont été remises en question en raison de la capacité des gouvernements à obtenir un accès légal aux données. Cet accès légal par le gouvernement est abordé au Québec, mais il ne sera pas un droit exerçable dans d'autres territoires de compétence.

Le principe de la responsabilité est à la base des transferts dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'OCDE[18] et également en vertu des lois canadiennes. Si le gouvernement a des préoccupations quant à la protection des Québécois, il serait optimal de répondre aux exigences par un mécanisme de reddition de comptes.

De plus, le manque d'équivalence attribuable à la question de l'utilisation par des gouvernements étrangers de données du secteur privé fondée sur une ordonnance légale devrait être abordé dans le cadre de discussions entre gouvernements. Il est déraisonnable et intenable d'imposer au secteur privé, en réponse à cette ordonnance, le fardeau de déterminer l'équivalence d'un cadre juridique « dans l'État où les renseignements seraient communiqués ». Selon le principe actuel de la responsabilité du Canada, les organisations doivent faire preuve de diligence en transférant des données et demeurer responsables de ces données ce faisant. Le gouvernement du Québec pourrait envisager de renforcer les exigences en matière de diligence raisonnable plutôt que de créer une exigence d'équivalence qui poserait problème.

La loi sur la protection des renseignements personnels devrait appliquer un principe de proportionnalité

Dans l'arrêt *R. c. Oakes*[19], la Cour suprême du Canada a établi le critère de proportionnalité. Il faut en tenir compte au moment de la rédaction des lois sur la protection des renseignements personnels. Par conséquent, voici les facteurs qui doivent être pris en compte :

> En premier lieu, l'objectif que doivent servir les mesures qui apportent une restriction à un droit garanti par la Charte doit être suffisamment important pour justifier de passer outre à un droit ou à une liberté garantis par la Constitution.

[17] *Le projet de loi 64 et l'exportation de données personnelles du Québec : des complications en vue*, Fasken, 17 août 2020. https://www.fasken.com/fr/knowledge/projet-de-loi-64/2020/08/17-the-exportation-of-personal-data-from-quebec

[18] https://www.oecd.org/fr/sti/ieconomie/privacy-guidelines.htm

[19] [1986] 1 RCS 103. https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/117/index.do

En deuxième lieu, la partie qui invoque l'article premier doit prouver que les moyens choisis sont raisonnables et que leur justification peut se démontrer. Cela nécessite l'application d'une sorte de critère de proportionnalité qui comporte trois éléments importants.

- D'abord, les mesures doivent être équitables et non arbitraires, être soigneusement conçues pour atteindre l'objectif en question, et avoir un lien rationnel avec cet objectif.
- De plus, le moyen choisi doit être de nature à porter le moins possible atteinte au droit en question.
- Enfin, il doit y avoir proportionnalité entre les effets de la mesure restrictive et l'objectif poursuivi – plus les effets préjudiciables d'une mesure sont graves, plus l'objectif doit être important.

Premièrement, pour les raisons exposées plus en détail ci-dessus, la section II du projet de loi, *Collecte de renseignements personnels*, est trop étroite et n'est donc pas soigneusement conçue pour atteindre l'objectif en question et n'a pas de lien rationnel à cet objectif – une loi sur la protection des renseignements personnels adaptée à l'ère numérique. Il est souvent impossible d'exiger le consentement pour la collecte de renseignements personnels à l'ère numérique, dans une économie axée sur l'information qui utilise l'ordinateur ou d'autres appareils technologiques comme moyen de communication[20]. Par conséquent, il est peu probable que le projet de loi sur la protection des renseignements personnels réponde efficacement à ce besoin.

De plus, le projet de loi ne porte pas aussi peu atteinte que possible au droit à la vie privée. Comme nous l'avons vu plus haut, le droit à la vie privée comporte de nombreux intérêts. Le recours excessif à l'un de ces intérêts, que ce soit l'autonomie ou le consentement, et l'absence de reconnaissance des autres intérêts, l'intimité et le traitement équitable, empêchent d'adopter une loi sur la protection de la vie privée adaptée à l'ère numérique.

Finalement, il n'y a pas de proportionnalité entre les effets et l'objectif. Comme nous l'avons vu plus haut, le droit à la vie privée n'est pas un droit absolu. Il faut tenir compte de la façon dont ce droit interagit avec d'autres droits et libertés. En particulier, il faut tenir compte de la nécessité pour les organisations de recueillir, d'utiliser et de communiquer des renseignements personnels. La disposition sur l'objet de la partie I de la LPRPDE[21] détermine la façon d'établir un équilibre entre le droit à la vie privée et le besoin des organisations de traiter les renseignements personnels :

> « La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »

[20] Adnan Rizal Harris, *Issues In Digital Era*, Research Gate, décembre 2016. https://www.researchgate.net/publication/328528038_Issues_In_Digital_Era/link/5bd275eba6fdcc3a8da64dd4/download

[21] https://laws-lois.justice.gc.ca/fra/lois/p-8.6/page-1.html#h-407066

Le projet de loi met trop l'accent sur la nécessité d'obtenir le consentement individuel à la collecte de renseignements personnels et sous-estime la nécessité pour l'entreprise de recueillir, d'utiliser et de communiquer des renseignements personnels à l'ère numérique.

Comme nous l'avons vu plus haut, il y a une façon moins lourde d'atteindre le même objectif. Il devrait y présenter une définition moderne de la responsabilisation. L'intérêt légitime ne doit pas se limiter à une exception au consentement et devrait être une base autonome bien définie pour la collecte, l'utilisation et la communication de renseignements personnels. L'équivalence des protections juridiques n'est pas la bonne structure de gouvernance pour les transferts – la responsabilisation l'est, et il devrait y avoir un équilibre proportionnel des droits et des libertés.

Une définition récente de la proportionnalité se trouve dans les lignes directrices canadiennes sur la COVID-19. Dans le *Cadre d'éthique en santé publique : Guide pour la réponse à la pandémie de COVID-19 au Canada*[22], il est énoncé ce qui suit sous *Réduire au minimum les préjudices* :

> « **Proportionnalité** : On doit soupeser les avantages potentiels et les risques de préjudice. Les mesures doivent être proportionnées à la menace et aux risques pertinents ainsi qu'aux avantages qui peuvent en découler. Si une limitation des droits ou des libertés est jugée essentielle pour atteindre un objectif, il convient de choisir les mesures les moins restrictives possible et de ne les imposer que dans la mesure nécessaire pour prévenir un préjudice prévisible. »

Compte tenu des avantages de l'économie numérique dont le gouvernement du Québec veut profiter, il est impératif que la proportionnalité entre les droits fondamentaux, et non la proportionnalité à l'intérieur d'un droit fondamental, soit équilibrée. Lorsqu'on établit un équilibre entre le droit à la vie privée et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels, il est clair que le projet de loi n'est pas proportionnel.

Conclusion

Il est difficile de rédiger un projet de loi sur la protection de la vie privée pour la prochaine génération. Il doit protéger tous les intérêts individuels tout en facilitant l'économie numérique. L'IAF est convaincue qu'un processus de consultation inclusif aboutira à une excellente loi. Son équipe se fera un plaisir de répondre à vos questions. Veuillez communiquer avec Martin Abrams à mabrams@informationaccountability.org.

[22] https://www.canada.ca/fr/sante-publique/services/maladies/2019-nouveau-coronavirus/reponse-canada/cadre-ethique-guide-reponse-pandemie-covid-19.html

10 September 2020

The Information Accountability Foundation ("IAF") appreciates the opportunity to comment on the proposed privacy legislation introduced by the Quebec government for passage in the Quebec National Assembly. The IAF is a global non-profit organization that conducts research and education on data protection and privacy from an accountability perspective. It is the incorporation of the Global Accountability Dialog that operationalized the accountability principle in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data for application in a digital economy and society.[1] The IAF has conducted research in Europe, Asia and the Americas, including three projects in Canada. The IAF conducted a dialog In Montreal on government use of data in 2014 with former Quebec privacy commissioner Jennifer Stoddart.[2] Next generation privacy legislation is an IAF focus area, and it is from that perspective that the IAF is providing these comments.

The IAF agrees with the Quebec government's assessment that now is the right time to update legislation enacted nearly thirty years ago. Quebec was an early Canadian adopter of private sector privacy law, enacting legislation in 1993. Quebec was a pathfinder because privacy is a fundamental right under the Quebec Charter of Human Rights and Freedoms and remains a fundamental right. Most fundamental rights are fairly straight forward. Not so privacy. In fact, scholars have a hard time capturing the essence of privacy in definitions. So, rather than define the right, it is often simpler to define the interests that the right encompasses. There are three interests:

- The first is the individual's interest in seclusion. All of us need a space where we are free of observation or intrusion into our private lives. This interest in seclusion rests on privacy within a household and the papers and the records associated with that household. In many ways our interest in seclusion has been eroded by the observational nature of modern society, where one may create a record of behavior without a legacy paper record.[3]
- The second is the individual's interest in defining his- or herself and not be defined by the digital tracks left behind. This is reflected in actions related to the individual's autonomy or ability to control the data that pertains to the reputation of the individual.[4]
- The third is the individual's interest in fair processing. This interest relates to the individual's interest in fair treatment, absent inappropriate discrimination, with decisions based on accurate data. As data has become fundamental to the way processes and machines work (e.g.

[1] https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

[2] "Organizational Accountability, Government use of Private Sector Data, National Security, and Individual Privacy."

[3] Section 5 of Chapter I of Part I of the Quebec Charter of Human Rights and Freedoms provides: "Every person has a right to respect for his private life."

[4] Section 4 of Chapter I of Part I of the Quebec Charter of Human Rights and Freedoms provides: "Every person has a right to the safeguard of his dignity, honour and reputation."

internet-of-things), more of the work of privacy agencies and privacy professionals has been dedicated to fair processing.[5]

How technology interfaces with those three interests is very different today than it was 30 years ago. The law predates the risks and benefits to people that have come with the Internet, smart phones, connected cars, advanced analytics and an internet of everything. When the enactment of privacy legislation is considered, how privacy intersects with other fundamental rights and interests needs to be considered. Privacy, while fundamental, is not an absolute right. Every individual has other rights and interests that are just as important. Those interests include better health and education, the right to be employed and create a business. They also include the right to information and to make decisions based on data validated facts. Sometimes those interests are best served when aggregated with the interests of other individuals into societal interests. For example, while an individual has an interest in how health records might impact reputation and standing, the individual also has an interest in that data being used in a protected manner for healthcare research. That interest in better healthcare through research is shared with all Quebeckers. Quality privacy law links one or more of those privacy interests and allows for proportionate balancing among all rights and freedoms.

While the IAF shares the view that the time is now for legislation, it believes the legislation could better balance the interests of all Quebeckers. The IAF's comments are all at a high level and suggest the proposed legislation should be structured with provisions that facilitate a vibrant society. In particular, the proposed legislation should be structured in a manner where the full range of rights and interests are addressed in a manner that matches remedies so that they tie proportionally with seclusion, autonomy, fair processing and other rights and interests. Proportionality is typically framed as an administrative requirement for government, where the fundamental rights of individuals are compromised by the power of the state as a user of data pertaining to people. Proportionality is different when framed as a private sector requirement. It links to advanced data users balancing the full range of interests of all stakeholders. While the emphasis is on the many interests of the individuals to whom the data pertains, the responsible data user also considers the interests of other stakeholders that may be impacted by the processing or failure to process data.

The Articulation of Accountability Should be Forward Thinking

The proposed legislation introduces the concept of accountability and very specifically sets forth how accountability should be achieved through specific and specified obligations. However, the legislation does not define purpose and true function for accountability. Accountability begins with the overarching principle that data should be processed by organizations in a responsible manner and should be answerable for that responsible processing.

The proposed legislation does not describe the overarching objective for accountability, and its provisions are both incomplete and too specific for a bill that is supposed to modernize the framework applicable to the protection of personal information. The Essential Elements of Accountability were

[5] Section 10 of Chapter I of Part I of the Quebec Charter of Human Rights and Freedoms provides: "Every person has a right to full and equal recognition and exercise of his human rights and freedoms, without distinction, exclusion or preference based on race, colour, sex, gender identity or expression, pregnancy, sexual orientation, civil status, age except as provided by law, religion, political convictions, language, ethnic or national origin, social condition, a handicap or the use of any means to palliate a handicap."

adopted by a global dialog in 2009[6] and are the basis for how accountability through a comprehensive privacy management program has been described in Canada.[7] This proposed legislation falls short when matched with the essential elements, as one can see in the chart below, much less modernize them for the decades ahead.

2009 Essential Elements of Accountability	Quebec Proposed Legislation
Organisation commitment to accountability and adoption of internal policies consistent with external criteria	The highest-ranking officer of the company is responsible for the protection of personal information, and the title and contact information of the person in charge ("PIC") must be published. Governance policies and practices that ensure the protection of personal information (i.e. retention and destruction of information, roles and responsibilities, complaints processes), proportionate to the nature and scope of activities, must be established, implemented, approved by the PIC and published on the enterprise's website.
Mechanisms to put privacy policies into effect, including tools, training and education	An assessment of the privacy-related factors of any information system or electronic service delivery project must be conducted. From the outset of the project, the PIC must be consulted. The project must allow computerized personal information to be communicated in a structured, commonly used technological format. The PIC may suggest personal information protection measures applicable to the project, such as: - Appointment of a person responsible for the implementing of personal information protection measures, - Measures to protect personal information in any document regarding the project, - Description of the project participants' responsibilities regarding the protection of personal information; - Training activities for project participants on the protection of personal information

[6] A representative of The Office of the Privacy Commissioner, Canada, participated in defining the essential elements of accountability.

[7] Getting Accountability Right with a Privacy Management Program, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/

Systems for internal, ongoing oversight and assurance reviews and external verification	
Transparency and mechanisms for individual participation	Governance policies and practices that ensure the protection of personal information (i.e. retention and destruction of information, roles and responsibilities, complaints processes), proportionate to the nature and scope of activities, must be established, implemented, approved by the PIC and published on the enterprise's website.
Means for remediation and external enforcement	
	If cause to believe that a confidentiality incident involving personal information has occurred exists, then reasonable measures to reduce the risk of injury and prevent new incidents of the same nature must be taken. - If the incident presents risk of serious injury, the following must be notified: - CAI - Person whose personal information is concerned - Any person or body that could reduce the risk may also be notified - In assessing the risk of injury, the following must be considered: - Sensitivity of the information concerned - Anticipated consequences of its use - Likelihood that information will be used for injurious purpose - Register of confidentiality incidents must be kept "Confidentiality incident" means: - Access not authorized by law to personal information, - Use not authorized by law of personal information, - Communication not authorized by law of personal information, or - Loss of personal information or any other breach in the protection of such information

As the above chart shows, the proposed legislation does not address all of the 2009 Essential Elements of Accountability, does not attempt to modernize the 2009 Essential Elements of Accountability, and for

the private sector, to a certain extent, duplicates the Digital Privacy Act amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA)[8] which introduced a mandatory data breach notification requirement

Modernizing Accountability for Quebec's Digital Future

As the digital strategy of Canada reveals, data drive national economies. The goal of Canada's digital strategy is for Canadians to benefit from the opportunities that the digital economy offers while at the same time protecting them from the threats posed by the embrace of digital technologies, including threats to the safety of personal data and to individual privacy.[9] In order for Quebeckers to benefit from this data driven age, Quebec needs an accountability framework that addresses and anticipates the benefits and detriments of digital technologies, especially those that operate without human involvement. This framework is known as Fair Processing Demonstrable Accountability which, among its requirements, includes an assessment process that balances the risk of harm and benefits to people of digital technologies. Digital technologies are electronic tools, systems, device and resources that generate, store or process data.[10] The IAF's work in Canada and other jurisdictions considers how the Essential Elements of Accountability might be updated for today's highly connected world. This work was featured in the Enhanced Data Stewardship EDIA project in partnership with the Privacy Commissioner of Hong Kong.[11] The IAF will be publishing further updated elements to address the elements of Fair Processing Demonstrable Accountability later in 2020. However, a summary version of these appears below. In short, , the accountability provisions of the proposed legislation do not come close to the requirements of Fair Processing Demonstrable Accountability. The accountability provisions of the proposed legislation provide a level of detail that does not address advances in technology, does not address the oversight and remediation necessary to make accountability successful and trusted, and take a narrow view of the scope of accountability.

For example, demonstrable accountability elements for a digital age should require:

- Organizational commitment to fair processing demonstrable accountability and the adoption of internal policies consistent with external criteria and established fair processing principles. As a matter of commitment, organizations should define fair processing values and/or principles which then are translated into organizational policies and processes. These principles should be organizationally derived and should be in addition to laws or regulations. They may go beyond what the law requires but should be aligned and not inconsistent with existing laws, regulations, or formal codes of conduct.
- Mechanisms to put fair processing policies into effect, including risk based adverse impact assessments, tools, training and education. Fair Processing Impact Assessments (FPIAs) should be required when advanced data analytics may impact people in a significant manner and/or when data enabled decisions are being made without the intervention of individuals. Where an analytical data driven use has potential impact at the individual level or at a higher level (e.g. groups of individuals and society), the benefits and adverse impacts should be explicitly defined

[8] https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html
[9] Canada's Digital Charter in Action: A Plan by Canadians, for Canadians, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html
[10] Education & Training, State Government of Victoria, Australia 2019
[11] https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Hong-Kong-Report-FINAL-for-electronic-distribution-10.22.18.pdf; https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Enhanced-Data-Stewardship-EDIA-FINAL-10.22.18.pdf

and should be mitigated to the extent possible. Organizations should use a "fair processing by design" process to translate their fair processing principles and other policy requirements into their digital technology system design processes so that society, groups of individuals, or individuals themselves, and not just the organizations, gain value from data processing activities.

- Internal review processes that assess higher risk FPIAs and the overall fair processing program. Higher risk or higher impacting data initiatives, or where adverse impacts have not been sufficiently addressed, should be referred to more senior organizational decision-making group(s) for their review and approval. The escalation process should be based on and be part of the programmatic risk management approach and should address that issues raised as part of the FPIA have been resolved and that advanced data processing activities have been conducted as planned.
- Individual and organizational transparency and mechanisms for individual participation. The fair processing principles that govern the advanced data processing activities and that underpin decisions should be communicated widely, and processes should be proactively transparent wherever possible. Furthermore, all societal and individual concerns should be addressed and documented as part of the FPIA process, and accountability feedback mechanisms should be established.
- Means for remediation and external enforcement. Organizations should stand ready to demonstrate to the regulatory agencies with authority, including certifying bodies to which the organizations are subject, the soundness of internal processes, the propriety of advanced data processing activities, and when data processing does or may impact people in a significant manner.

The failure of the proposed legislation to address any of these elements of demonstrable accountability for digital technologies means that the proposed legislation is outdated before it is even passed. The proposed legislation is asking both the public and private sectors to use scarce resources to put in place processes that do not address the digital challenges of today and the future.

The Lawful Collection of Personal Information Should Not be Limited to Consent

In the 2016-2017 Report on Consent of the Office of the Privacy Commissioner, it was recognized that consent may be a poor fit in certain circumstances, e.g., where consumers do not have a relationship with the organization using their data and where uses of personal data are not known at the time of collection, or too complex to explain to individuals. Consent is a foundational element of PIPEDA. Legally, organizations must obtain meaningful consent to collect, use and disclose an individual's personal information, subject to certain exceptions. When PIPEDA was adopted, interactions with businesses were generally predictable, transparent and bidirectional. Individuals understood why the company they were dealing with needed certain personal information. There were clearly defined moments when information collection took place and consent was obtained. But obtaining consent has become increasingly challenging and ineffective in protecting individuals in the digital environment. While there remains an important role for consent in protecting the right to privacy where it can be meaningfully given, complex information flows and business processes involving a multitude of third-party intermediaries, such as search engines, platforms, and advertising companies, have put a strain on the consent model; in the age of big data, the Internet of Things, artificial intelligence and robotics, it is no longer entirely clear to consumers who is processing their data and for what purposes; for individuals, the cost of engaging with modern digital services means accepting, at some level, that their personal information will inevitably be required to be collected and used by companies in exchange for a

product or service.[12] Given the recognition that business relationships are no longer just bidirectional and that consent may no longer always be practicable, it is outdated to draft legislation that is supposed to be modernizing to require consent as a condition to collect personal information from the individual.

Arguing that personal information may also be collected from a third person if there is a serious and legitimate reason does not work because either of the following conditions must be fulfilled: (1) the information is collected in the interest of the person concerned and cannot be collected from him in due time, or (2) collection from a third person is necessary to ensure the accuracy of the information. In other words, there are only two legitimate reasons. This provision is way too limiting to be a useful legitimate interest provision.

Given that the proposed legislation appears to try and incorporate many of the elements of the EU General Data Protection Regulation ("GDPR), it would be prudent to also incorporate the legitimacy of data processing set forth in Article 6 of the GDPR. This Article contains six legal means to process data, one of which is legitimate interests. Legitimate interest in the GDPR is much broader than legitimate reason in the proposed legislation. Legitimate interest concerns processing "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[13] The recitals to the GDPR make clear that the processing of personal data strictly for the purposes of preventing fraud constitutes a legitimate interest of the data controller concerned, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest, where controllers are part of a group of undertakings or institutions affiliated to a central body, they may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data.[14] The recitals make it clear that the processing described in them are examples and that other circumstances that meet the requirements of the GDPR are permitted, i.e., those necessary for the purposes of the legitimate interests pursued by the controller or by the third party AND those not overridden by the interests or fundamental rights and freedoms of the data subject.[15] How legitimate interests is approached in the GDPR demonstrates how narrow, unworkable and outdated legitimate reason is in the Quebec proposed legislation.

Equivalency of Legal Protections is Not the Right Structure for Transfers of Personal Information

The proposed legislation provides that before communicating personal information outside Quebec, an assessment of privacy-related factors must be conducted taking into account:

1. The sensitivity of the information;
2. The purposes for which it is to be used;
3. The protection measures that would apply to it; and
4. The legal framework applicable in the State in which the information would be communicated, including the legal framework's degree of equivalency with the personal information protection principles applicable in Quebec.

[12] 2016-2917 Report on Consent. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1
[13] GDPR Article 6(e)
[14] GDPR Recitals 47 and 48
[15] GDPR Recital 47

The information may be communicated if the assessment establishes that it would receive protection equivalent to that afforded under the proposed legislation.[16] If this standard is not met, no transfer is allowed. Such a limited transfer mechanism is economically unviable, is destructive to businesses located in Quebec and to Quebec's economy in general, is isolationistic, and is not the kind of modernization called for by this proposed legislation.

This proposed legislation is intended to regulate both the private and public sector's communication of personal information in Quebec and personal information that has its origin in Quebec but might be communicated in another jurisdiction. Achieving domain over data through time and space has been a dilemma since the first privacy law. Canada has chosen to regulate privacy in a federal manner with oversight and enforcement duties shared between the federal government and the provinces. Just as in Europe, this approach means all jurisdictions that are party to the system are considered competent to fulfill their respective role. The proposed legislation, and its requirement for equivalent protections in other jurisdictions, does not make it clear that other Canadian jurisdictions, by membership in this federal system, are competent and therefore equivalent. If that is not the case, it has practical implications for how businesses operate. For example, it would be unfortunate if a supervisor would not have the data to oversee an employee in Quebec because his or her Canadian province had a law that accomplishes similar objectives but was not equivalent in structure.

The same could be said for transfers beyond Quebec. Many Quebeckers conduct business in other countries. Many are employed by companies in the United States, for example. In 2019, of Quebec's exports, 71.2% went to the United States.[17] Equivalency (under the name adequacy but defined as equivalency) for transfers has been built into the European private sector privacy law, the GDPR. However, Europe has only been able to find a handful of jurisdictions as adequate, and all are up for review by the European Commission. Fortunately, the GDPR allows for derogations where a company can assure European data will be protected at European standards by data controllers. However, even those derogations have been brought into question because of the ability for governments to get lawful access to data. That lawful access by government is addressed in Quebec but will not be exercisable in other jurisdictions.

Accountability is the basis for transfers in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[18] and has been the basis under Canadian law. If the government has concerns about protecting Quebeckers, it would be optimal to address the requirements through an accountability mechanism.

Further, the lack of equivalency due to the question of foreign governments' use of data from the private sector based on a lawful order should be addressed by government to government discussions. Putting the burden of determining the equivalency of a legal framework "in the State in which the information would be communicated" on the private sector that must respond to a lawful order is unreasonable and untenable. Canada's current accountability principle requires organizations to be diligent when transferring data and to stay responsible for that data when doing so. The Quebec

[16] Section 17

[17] Bill 64 and The Exportation of Personal Data from Quebec: Complications in Sight, Fasken, August 17, 2020. https://www.fasken.com/en/knowledge/projet-de-loi-64/2020/08/17-the-exportation-of-personal-data-from-quebec

[18] https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

government might consider enhancing the requirements for due diligence rather than create an equivalency requirement that would be problematic.

Privacy Legislation Should Be Proportionate

In *R. v. Oakes,*[19] the Supreme Court of Canada set forth the proportionality test. This test should be considered when drafting privacy legislation. Thus, the following factors should be considered:

> First, the objective to be served by the measures limiting a Charter right must be sufficiently important to warrant overriding a constitutionally protected right or freedom.
>
> Second, the party invoking the first section must show the means to be reasonable and demonstrably justified. This involves a form of proportionality test involving three important components.
>
> - To begin, the measures must be fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective.
> - In addition, the means should impair the right in question as little as possible.
> - Lastly, there must be a proportionality between the effects of the limiting measure and the objective – the more severe the deleterious effects of a measure, the more important the objective must be.

First, for reasons discussed in more detail above, Division II of the proposed legislation, Collection of Personal Information, is overly narrow and therefore is not carefully designed to achieve the objective in question and is not rationally connected to that objective - a privacy law suitable for the digital age. Requiring consent for the collection of personal information in the digital age, an information-based economy using computer or other technology devices as medium or communication,[20] is often impossible. Therefore, this proposed privacy law is unlikely to be effective in meeting that need.

In addition, the proposed legislation does not impair the right to privacy as little as possible. As also discussed above, the right to privacy consists of many interests. Over reliance on one of those interests, autonomy or consent, and no recognition of the other interests, seclusion and fair processing, impedes the ability to achieve a privacy law suitable for a digital age.

Lastly, there is no proportionality between the effects and the objective. As further discussed above, privacy is not an absolute right. There must be consideration of how privacy interacts with other rights and freedoms. In particular, there must be a consideration of the need of organizations to collect, use and disclose personal information. The Purpose provision of Part I of PIPEDA[21] sets forth how to balance the right of privacy and the need of organizations to process personal information:

> "The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of

[19] [1986] 1 SCR 103. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/117/index.do
[20] Adnan Rizal Harris, Issues in Digital Era, Research Gate, December 2016 https://www.researchgate.net/publication/328528038_Issues_In_Digital_Era/link/5bd275eba6fdcc3a8da64dd4/download
[21] https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html#h-416888

> personal information in a manner that recognizes the right of privacy of individuals and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

The proposed legislation overemphasizes the need for individual consent to the collection of personal information and underemphasizes the enterprise's need to collect, use and disclose personal information in the digital age.

As discussed above, there is a less privacy invasive way of achieving the same end. There should be a modern articulation of accountability; legitimate interest should not be limited to an exception to consent and should be a well-articulated standalone basis for collecting, using and disclosing personal information; equivalency of legal protections is not the right governance structure for transfers – accountability is; and there should be a proportionate balancing of rights and freedoms.

A recent articulation of proportionality is found in the Canadian guidance on COVID-19. In the Public health ethics framework: A guide for use in response to the COVID-19 pandemic in Canada,[22] it is stated under Minimizing Harm:

> "**Proportionality**: potential benefits should be balanced against the risks of harm. Measures should be proportionate to the relevant threat and risks, and the benefits that can be gained. If a limitation of rights, liberties or freedoms is deemed essential to achieve an intended goal, the least restrictive measures possible should be selected, and imposed only to the extent necessary to prevent foreseeable harm."

Given the benefits of the digital economy that the Quebec Government wants to take advantage of, it is imperative that proportionality among fundamental rights, and not proportionality within a fundamental right, is balanced. When balancing the right of privacy and the need of organizations to collect, use or disclose personal information, it is clear that the proposed legislation is not proportionate.

Concluding Remarks

Writing privacy legislation for the next generation is difficult. It must protect the full range of individual interests but still facilitate a digital economy. The IAF is confident that with an inclusive consultation process, quality legislation will be the outcome. The IAF team would be pleased to respond to questions. Please reach out to Martin Abrams at mabrams@informationaccountability.org.

[22] https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection/canadas-reponse/ethics-framework-guide-use-response-covid-19-pandemic.html