CENTRE FOR DIGITAL RIGHTS
CENTRE POUR LES DROITS NUMÉRIQUES

Ne convient pas à l'objet – Le Canada mérite beaucoup mieux

Rapport du Centre pour les droits numériques sur le projet de loi C-27

Loi de 2022 pour la mise en oeuvre de la Charte numérique du Canada

Première publication le 28 octobre 2022
Mis à jour le 2 octobre 2023*

* Sous réserve de changements – 1) après que le ministre d'Innovation, Sciences et Développement économique Canada (ISDE) ait publié les modifications proposées au projet de loi C-27 dont il est question dans sa comparution devant le Comité permanent de l'industrie, des sciences et de la technologie (INDU) le 26 septembre 2023 et 2) avant que le Centre pour les droits numériques (CDN) ne comparaisse devant l'INDU.

Le Centre pour les droits numériques (CDN) est une organisation canadienne non partisane à but non lucratif qui vise à sensibiliser le public aux problèmes numériques liés à l'économie axée sur les données a) en faisant mieux comprendre au public ses droits, b) en améliorant la compréhension des décideurs politiques en matière de technologie de pointe et c) en faisant la promotion de meilleures pratiques, de lois et de réglementations qui protègent à la fois les valeurs civiques et les droits des personnes dans l'économie du vingt-et-unième siècle, une économie portée par la collecte, l'utilisation et la divulgation massives de données.

Préface de la mise à jour du 2 octobre 2023

Ce rapport du CDN sur le projet de loi C-27 développe et met à jour la déclaration du CDN concernant le projet de loi C-27 publiée le 28 octobre 2022.

Ce rapport mis à jour :

- vise à tenir compte d'une réflexion plus approfondie et de faits importants récents concernant la législation proposée sur la protection des renseignements personnels et sur l'intelligence artificielle (IA) dans le secteur privé « adaptée à l'usage », qui se sont produits depuis l'automne 2022, tant au Canada qu'à l'étranger. Plus précisément, le présent rapport traite des éléments résumés à l'annexe H ;
- se fonde sur la version du projet de loi C-27 qui a franchi l'étape de la deuxième lecture le 24 avril 2023. À ce jour, il s'agit de la version publiée de la législation proposée ;
- ne tient pas compte et ne peut pas tenir compte des amendements en principe proposés que le ministre ISDE François-Philippe Champagne a mentionnés dans son témoignage devant le Comité INDU le 26 septembre 2023 et dont il a indiqué qu'ils ne seraient fournis au Comité INDU qu'après le début de son examen article par article du projet de loi C-27 (c'est-à-dire, curieusement, après la présentation des témoins[1]), y compris notamment :
    - faire du respect de la vie privée un droit fondamental ;
    - prévoir des règles plus strictes en matière de protection de la vie privée des enfants ;
    - donner au commissaire à la protection de la vie privée du Canada une marge de manoeuvre accrue pour conclure des accords de conformité ;
    - définir des catégories de systèmes d'IA qui seraient considérées comme ayant une incidence élevée ;
    - donner plus de précisions au nouveau commissaire aux données.

Face à ces circonstances inhabituelles, le CDN 1) s'oppose au manque de transparence du gouvernement dans son approche du travail important que le Comité INDU doit accomplir pour étudier le projet de loi C-27 et 2) réserve ses commentaires sur le texte juridique réel de ces amendements gouvernementaux promis, mais non encore publiés jusqu'à ce qu'ils aient été rendus publics comme l'exigent généralement les principes de bonne gouvernance démocratique et plus précisément la motion adoptée par le Comité INDU le 28 septembre 2023.[2]

1. Le 27 septembre 2023, le professeur Michael Geist a dénoncé le gouvernement fédéral pour cette manoeuvre secrète dans son blogue intitulé *Why Industry Minister Champagne Broke the Bill C-27 Hearings on Privacy and AI Regulation in Only 12 Minutes* (« Pourquoi le ministre de l'Industrie Champagne a interrompu les audiences sur le projet de loi C-27 sur la protection des renseignements personnels et la réglementation sur l'IA après seulement 12 minutes »). Les députés conservateurs, néo-démocrates et bloquistes de l'opposition siégeant au Comité INDU ont imploré le ministre de déposer les amendements du gouvernement lors de la réunion du 26 septembre ou dans un avenir très proche.
2. Le texte de cette motion se lit ainsi : « Que, conformément au paragraphe 108(1) du Règlement, le Comité ordonne au ministre et à son Ministère de produire les amendements discutés par le ministre dans ses remarques préliminaires au Comité le 26 septembre 2023, à condition que ces documents soient déposés auprès du greffier du Comité dans les cinq jours ouvrables et que le ministre revienne pour s'exprimer à leur sujet ». Le CDN interprète cette motion comme signifiant que le ministre doit fournir les amendements proposés par l'ISDE à l'INDU d'ici le 4 octobre 2023.

TABLE DES MATIÈRES

Page

Résumé

On s'entend généralement pour dire que la *Loi sur la protection des renseignements personnels et les documents électroniques* (**LPRPDE**) a expiré et qu'il est urgent de la mettre à jour. Le projet de loi C-27, *Loi de 2022 d'exécution de la Charte canadienne du numérique*, tente de s'attaquer à la réglementation s'appliquant au secteur privé en matière de protection des renseignements personnels en présentant trois projets de loi : la *Loi sur la protection des renseignements personnels des consommateurs (***LPRPC***), la Loi sur le Tribunal de la protection des renseignements personnels et* des *données (LPRPDE) et la Loi sur l'intelligence artificielle et les données* (**LIAD**). Malheureusement, dans sa forme actuelle, le projet de loi C-27 rate l'occasion de produire une loi d'avant-garde qui tient compte des risques énormes et des asymétries que présente le modèle d'affaires actuel de la surveillance.

Il y a vingt ans, la Commission européenne a jugé que le Canada offrait un « niveau de protection adéquat », du moins pour les entreprises visées par la LPRPDE, permettant ainsi que des données personnelles soient transmises au Canada sans qu'aucune autre mesure de protection ne soit nécessaire. Le seuil a maintenant changé en raison des jugements des tribunaux européens et d'une loi européenne historique et novatrice de 2018, le Règlement général sur la protection des données (**RGPD**). Il est d'une importance capitale pour les entreprises canadiennes que le jugement sur le caractère adéquat ne soit pas annulé. Le jugement sur le caractère adéquat est un jugement formel, et il peut impliquer les décisions de plusieurs institutions et juridictions européennes. Le Canada ne devrait pas présumer que notre statut sera maintenu simplement parce que nous l'avons déjà obtenu avec la LPRPDE.

Les Canadiens se soucient aussi de leur vie privée. Dans un sondage mené récemment[3], 93 % des Canadiens ont exprimé des préoccupations au sujet de la protection de leur vie privée. Les Canadiens sont moins nombreux à penser que les entreprises respectent leurs droits en matière de protection des renseignements personnels, et seulement un Canadien sur 10 fait confiance aux sociétés de médias sociaux pour protéger ses renseignements personnels.

En consultation avec certains des plus grands experts et leaders d'opinion du Canada en matière de protection de la vie privée, le Centre pour les droits numériques (**CDN**) a préparé le présent rapport concernant le projet de loi C-27, recommandant de **rendre le projet de loi C-27 apte à relever les défis actuels en matière de protection de la vie privée au Canada et conforme aux normes mondiales contemporaines en matière de protection de la vie privée.** Ce rapport vise à aider à remédier aux lacunes du projet de loi C-27, ce qui est essentiel, en s'inspirant de l'historique d'innovation du Canada en matière de protection de la vie privée et d'exemples provenant d'autres administrations de premier plan. Il contient des recommandations précises visant à faire en sorte que la LPVPC proposée soit adaptée aux défis actuels et futurs, et met en lumière les préoccupations liées à l'adoption à la hâte de mesures législatives inutiles (LTPRPD) et inadéquates (LIAD).

[3] Commissariat à la protection de la vie privée du Canada, *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2022-2023* (mars 2023), en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2023/por_ca_2022-23/

Voici les principales recommandations du CDN pour corriger le projet de loi C-27 :

- La LPVPC devrait **reconnaître la vie privée comme un droit fondamental de la personne** inextricablement lié à d'autres droits et libertés fondamentaux. En tant que droit de la personne, il ne convient pas de « concilier » le droit à la vie privée et les intérêts commerciaux, bien que toute perte du droit à la vie privée devrait être conciliée avec d'autres droits fondamentaux, comme le droit à la liberté d'expression.

- La LPVPC devrait **aborder les risques liés à la vie privée pour la démocratie** et étendre la portée de la LPVPC pour couvrir les partis politiques fédéraux (**PPF**) du Canada. C'est le comble du cynisme et de l'hypocrisie que les PPF continuent de faire fi des recommandations des commissaires à la protection de la vie privée au Canada et à l'étranger, du comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique (le **Comité ETHI**), des experts en matière de protection de la vie privée et de gouvernance des données, des défenseurs et des sondages d'opinion publique visant à inclure expressément les PPF dans la loi fédérale sur la protection de la vie privée du secteur privé, puis de demander à toutes les autres organisations de suivre des règles que les PPF refusent de suivre eux-mêmes. La récente modification de la *Loi électorale du Canada* par le gouvernement fédéral, qui prétend adopter une approche uniforme et exclusive de la façon dont les PPF protègent la vie privée des Canadiens, est à la fois hypocrite et contraire à la Constitution du Canada (« **Constitution du Canada** ») et à la Charte canadienne des droits et libertés (la « **Charte** »). Dans le cadre d'observations distinctes présentées au Comité sénatorial permanent des affaires juridiques et constitutionnelles le 3 mai 2023 (voir l'annexe G pour plus de détails), le commissaire à la protection de la vie privée du Canada et le directeur général des élections du Canada ont tous les deux décrit cette modification (qui n'était alors qu'une proposition) comme étant inadéquate pour protéger les renseignements personnels des Canadiens et contraire à leurs recommandations visant à imposer de véritables obligations en matière de protection de la vie privée dans les PPF.

- Le gouvernement fédéral devrait **consulter efficacement les peuples autochtones et reconnaître leur souveraineté en matière de données.** Son défaut de le faire est incompatible avec l'obligation du gouvernement fédéral de mettre en œuvre la *Déclaration des Nations Unies sur les droits des peuples autochtones.* Cette situation est inacceptable et inexcusable, surtout à la lumière des principes de propriété, de contrôle, d'accès et de possession (« principes de PCAP® ») des Premières Nations. Les voix autochtones ne doivent pas être laissées de côté si le gouvernement fédéral veut sérieusement établir une base de confiance dans le monde numérique au Canada.

- La portée de protection de la vie privée devrait être étendue pour tenir **compte des risques pour la vie privée des groupes et des personnes**. La LPVPC devrait étendre la protection aux groupes suffisamment définis comme les ménages et les enfants dans une salle de classe. Les « renseignements sensibles » devraient être définis de façon appropriée dans la loi et les mineurs devraient être mieux protégés par des exigences de confidentialité spéciales et renforcées.

- Les **dispositions sur le consentement de la LPVPC doivent être corrigées**, puisque la LPVPC a éliminé un important libellé sur le consentement qui se trouvait dans la LPRPDE et a omis les garde-fous nécessaires pour assurer des protections adéquates de

la vie privée qui placent clairement les intérêts et les droits fondamentaux d'une personne au-dessus des intérêts commerciaux de l'organisation. Un consentement explicite doit être demandé relativement aux médias numériques pour la collecte, l'utilisation ou à la divulgation de renseignements personnels à des fins autres que celles qui sont nécessaires pour fournir un produit ou un service. Cette forme de consentement devrait être dissociée des conditions d'utilisation et ne pas constituer une condition de la fourniture des produits ou de la prestation des services. Les articles 15 et 18 (concernant l'intérêt légitime) de la LPVPC devraient être réécrits.

- La LPVPC devrait **utiliser tous les outils de la « boîte à outils de protection de la vie privée et des consommateurs » pour favoriser la responsabilité**. Il s'agit notamment d'exiger des évaluations des facteurs relatifs à la vie privée (**EFVP**) avant l'utilisation de technologies envahissantes ou le traitement à risque élevé, d'établir des exigences en matière de protection de la vie privée par défaut, de promouvoir l'élaboration de modèles d'intendance des données, d'imposer des exigences supplémentaires concernant les flux de données transfrontaliers et d'établir un régime plus complet régissant les tiers fournisseurs de services et de traitement de données.

- La LPVPC devrait **renforcer le contrôle des personnes sur leurs renseignements personnels (RP)**, par exemple en accordant un droit plus complet à la mobilité ou à la transférabilité des données et en limitant les exceptions au droit d'éliminer des RP.

- La LPVPC devrait **donner plus de mordant au Commissariat à la protection de la vie privée.** La LPVPC devrait doter le commissaire à la protection de la vie privée d'approches d'application plus souples et de pouvoirs lui permettant d'imposer des sanctions administratives pécuniaires. **La LTPRPD devrait être supprimée**. Aucune justification (innovation en droit de protection de la vie privée ou autre) n'a été donnée pour un tel tribunal. Son rôle et sa composition soulèvent de sérieuses préoccupations (notamment une complexité, des délais et de l'incertitude inutiles pour les personnes et les organisations dans le règlement d'une plainte. De plus, aucun régime de droit en matière de protection de la vie privée au monde n'a établi un tribunal comme le Tribunal proposé en vertu de la LTPRPD (y compris les régimes modernes et progressistes de l'UE et de la Californie, ainsi que les régimes de l'Utah, du Colorado, de la Virginie et du Connecticut, et le projet de loi américain qui s'intitule *American Data Privacy and Protection Act*). Ce tribunal n'est pas non plus proposé dans le *Privacy Act Review Report 2022* du 16 février 2023 du gouvernement australien.

- **La LIAD devrait être renvoyée à la table à dessin, mais pas à ISDE seulement**. Elle est inappropriée et incomplète et met l'accent de manière excessive sur les risques de préjudice pour les « personnes » plutôt que sur les préjudices pour les « groupes et les collectivités ») (aussi appelés les préjudices « collectifs ».

Le Canada devrait saisir l'occasion qui se présente d'apprendre des meilleures normes mondiales actuelles en matière de protection des données, d'élaborer une loi d'avant-garde et de réellement « moderniser » ses lois (y compris en élaborant et en mettant en œuvre un nouveau cadre de gouvernance rigoureux en matière de *contrôle dès la conception*). Malheureusement, le projet de

loi C-27 n'est pas conforme aux normes mondiales contemporaines. Il ne permet pas de régler les graves problèmes de protection de la vie privée qui ont surgi depuis l'adoption de la LPRPDE. Plus important encore, il ne tient pas compte du fait que les entreprises dominantes axées sur les données ont délaissé leur modèle d'affaires axé sur les services pour adopter un modèle qui repose sur la monétisation des renseignements personnels (RP) par la surveillance de masse de personnes et de groupes.

À propos des experts du CDN consultés*

** La contribution non rémunérée, volontaire et significative de chaque expert au présent rapport est grandement appréciée.*

Dr Colin Bennett

Colin Bennett est professeur émérite de sciences politiques à l'Université de Victoria, en Colombie-Britannique, et chercheur associé au Centre for Global Studies. Pendant plus de trente ans, ses recherches ont porté sur l'incidence des technologies de surveillance et sur l'analyse comparative de la gouvernance de la protection de la vie privée aux niveaux national et international. En plus de nombreux articles de journaux et universitaires, il a publié sept livres sur ces sujets, dont *The Governance of Privacy* (MIT Press, 2006), ainsi que des rapports sur les politiques d'organisations nationales et internationales, dont le Commissaire à la protection de la vie privée du Canada, la Commission européenne, le Conseil de l'Europe et l'*Information Commissionner's Office* du Royaume-Uni. Il étudie actuellement la saisie et l'utilisation des données personnelles des électeurs par les partis politiques dans les démocraties occidentales. Pour plus d'informations, veuillez consulter son site Web : https://www.colinbennett.ca/

Dr André Clément

Dr Andrew Clement est professeur émérite à la Faculté d'information de l'Université de Toronto, où il coordonne l'*Information Policy Research Program*. Il a cofondé le *Identity Privacy and Security Institute*. Titulaire d'un doctorat en informatique, il s'intéresse depuis longtemps à la recherche et à l'enseignement dans les domaines de l'implication sociale des technologies de l'information et des communications, de la conception participative, de la surveillance et de la protection des renseignements personnels. Ses projets récents se sont axés sur la promotion de la transparence et de la responsabilité concernant la surveillance basée sur Internet.

Dr Teresa Scassa

Dr Teresa Scassa est titulaire de la Chaire de recherche du Canada en droit et politiques de l'information à la Faculté de droit de l'Université d'Ottawa. Elle est membre du Conseil consultatif en matière d'intelligence artificielle et a été membre du Comité consultatif externe du Commissariat à la protection de la vie privée du Canada. Elle a été nommée première chercheuse en résidence au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario pour une période allant de septembre 2022 à juin 2023. Elle a beaucoup écrit dans les domaines du droit de la vie privée, de la technologie (y compris l'intelligence artificielle) et de la propriété intellectuelle. Pour plus d'informations, veuillez visiter son blog à : http://www.teresascassa.ca

A. Introduction

On s'entend généralement pour dire que la *Loi sur la protection des renseignements personnels et les documents électroniques* (**LPRPDE**) a expiré et qu'il est urgent de la mettre à jour. À cet égard, la *Loi de 2022 sur la mise en œuvre de la Charte du numérique* proposée par le gouvernement fédéral (**projet de loi C-27**) est une bonne nouvelle. Malheureusement, le projet de loi C-27, tel qu'il est présenté, rate l'occasion de produire une loi d'avant-garde qui tient compte des risques énormes et des asymétries que présente le modèle d'affaires actuel de la surveillance.

Le projet de loi C-27 tente de s'attaquer à la réglementation sur la protection des renseignements personnels s'appliquant au secteur privé en présentant trois projets de loi : la *Loi sur la protection des renseignements personnels des consommateurs* (**LPRPC**), la *Loi sur le Tribunal de la protection des renseignements personnels et des données* (**LTPRPD**) et la *Loi sur l'intelligence artificielle et les données* (**LIAD**). Le projet de loi C-27 corrige certaines des lacunes les plus flagrantes du régime de réglementation « peu contraignant » de la LPRPDE, notamment en accordant au commissaire à la protection de la vie privée du Canada le pouvoir de rendre des ordonnances exécutoires et de recommander l'imposition de sanctions administratives pécuniaires dans certaines circonstances, mais en même temps, il affaiblit certaines mesures de protection des données.

Ce manque de cohérence a amené l'ancien commissaire à la protection de la vie privée du Canada, Daniel Therrien, à qualifier le prédécesseur du projet de loi C-27, l'ancien projet de loi C-11, de « recul général en matière de protection de la vie privée »[4]. Malheureusement, le projet de loi actuel, dans l'ensemble, ne fait pas mieux. Bien que l'actuel commissaire à la protection de la vie privée du Canada, Philippe Dufresne, déclare, à propos du projet de loi C-27, qu'il « s'agit, à bien des égards, d'une amélioration par rapport à la LPRPDE et à l'ancien projet de loi C-11 » et que c'est donc un « pas dans la bonne direction », il s'empresse de souligner dans le mémoire du CPVP sur le projet de loi C-27 daté d'avril 2023 que celui-ci « peut être amélioré davantage et doit l'être »[5]. Le projet de loi C-27 ne permet pas de régler les graves problèmes de protection de la vie privée qui ont surgi depuis l'adoption de la LPRPDE. Plus important encore, il ne tient pas compte du fait que les entreprises dominantes axées sur les données ont délaissé leur modèle d'affaires axé sur les services pour adopter un modèle qui repose sur la monétisation des renseignements personnels au moyen de la surveillance de masse de personnes et de groupes. Ce modèle légèrement réglementé s'est révélé extrêmement lucratif, produisant une nouvelle génération de géants de la technologie d'une taille et d'une portée sans précédent et exacerbant les asymétries de pouvoir que ces organisations expérimentaient déjà avec les personnes concernées (tant les personnes que les groupes).

---

[4] Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, mai 2021, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_ethi_c11_2105/

[5] Commissariat à la protection de la vie privée du Canada, « Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-27, la Loi de 2020 sur la mise en œuvre de la Charte du numérique », 2022, avril 2023, en ligne : https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_indu_c27_2304/

Le projet de loi proposé ne correspond pas non plus aux normes mondiales contemporaines ni à la réalité actuelle de la circulation des renseignements personnels. Bien que la LPRPDE ait passé un « test de suffisance » il y a une vingtaine d'années, en vertu de la Directive sur la protection des données personnelles de l'Union européenne, le Parlement ne devrait pas présumer que le projet de loi C-27 respectera la norme plus élevée d'« équivalence substantielle » en vertu du *Règlement général sur la protection des données* (**RGPD**) de l'Union européenne, qui est plus rigoureux. Il est d'une importance capitale pour les entreprises canadiennes et pour les Canadiens que l'on maintienne le caractère « adéquat » de la mesure. Les Canadiens se soucient aussi de leur vie privée. Dans un sondage récent, 93 % des Canadiens ont exprimé des préoccupations au sujet de la protection de leur vie privée. Les Canadiens sont moins nombreux à penser que les entreprises respectent leurs droits en matière de protection des renseignements personnels, et seulement un Canadien sur 10 fait confiance aux sociétés de médias sociaux pour protéger ses renseignements personnels[6].

Il est donc de plus en plus urgent que les législateurs en matière de protection des données corrigent ces lacunes et fournissent aux Canadiens un moyen efficace de faire valoir leur droit à la vie privée et de tenir les organisations responsables de leurs actes. Le présent rapport a pour but d'aider à cette tâche essentielle. En s'inspirant de l'historique d'innovation du Canada en matière de protection de la vie privée et d'exemples provenant d'autres administrations de premier plan, ce document propose des recommandations précises (y compris, pour une étude plus approfondie, une recommandation visant la mise en œuvre d'un nouveau cadre de gouvernance rigoureux de *contrôle par conception*) pour que la LPVPC proposée soit adaptée aux défis actuels et futurs, et met en lumière les préoccupations liées à l'adoption à la hâte de mesures législatives inutiles (LTPRPD) et inadéquates (LIAD).

B. Recommandations visant à corriger les problèmes du projet de loi C-27 et à le rendre adapté à son objet

1. Faire en sorte que le projet de loi C-27 réponde aux défis actuels en matière de protection des renseignements personnels et soit conforme aux normes mondiales actuelles en la matière

Le projet de loi C-27 devrait s'harmoniser davantage avec le RGPD afin que le Canada soit reconnu comme un pays doté de règles adéquates en matière de protection des données personnelles.

> Le Canada était autrefois perçu comme un pionnier et reconnu pour son avant-gardisme en matière de protection de la vie privée contre les pires abus des technologies numériques. Malheureusement, le projet de loi C-27 n'est pas conforme aux normes mondiales contemporaines. En effet, les idées et les outils stratégiques, dont il sera question ci-dessous, qui ont été mis au point au Canada et exportés vers d'autres pays, ne figurent pas dans le projet de loi C-27. Le gouvernement a raté une occasion en or d'élaborer une loi

[6] Commissariat à la protection de la vie privée du Canada, *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2022-2023* (mars 2023), en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2023/por_ca_2022-23/

d'avant-garde, qui répondrait aux énormes risques que posent le capitalisme de surveillance et les modèles d'affaires qu'il inspire et appuie.

Les données personnelles circulent partout dans le monde, mais en lisant ce projet de loi, on ne le saurait pas. Contrairement à d'autres lois contemporaines sur la protection des renseignements personnels, il n'y a pas d'article spécifique qui clarifie les règles relatives au transfert de données personnelles à l'extérieur du Canada (le chapitre 5 du RGPD contient sept articles distincts sur cette question). La *Loi 25* du Québec (anciennement le projet de loi 64), traite également de ces questions plus en détail que le projet de loi C-27. Comme il est indiqué ci-dessous, il s'agit d'une lacune importante de la législation fédérale proposée qui doit être corrigée pour les Canadiens et les entreprises canadiennes. Il s'agit également d'une lacune qui pourrait menacer une évaluation du caractère adéquat en vertu du droit européen.

Qu'on le veuille ou non, le RGPD est généralement considéré comme la norme mondiale *de facto* pour la protection des données internationales. Il est courant dans les milieux d'affaires que le RGPD soit trop normatif, fondé sur des règles et descendant[7]. Ce récit contraste supposément avec l'approche bureaucratique européenne et les approches plus souples « fondées sur des principes » sur lesquelles reposent la LPRPDE et maintenant le projet de loi C-27. Il s'agit d'une fausse dichotomie. Le RGPD maintient toute la souplesse nécessaire pour permettre aux entreprises de traiter les données personnelles en fonction de leurs besoins légitimes. L'affirmation selon laquelle le RGPD, et le droit européen en général, étouffe l'innovation ne repose sur aucune preuve. C'est un mythe (voir le résumé des recherches à l'annexe « D »). Nous devrions rejeter l'argument selon lequel cette approche « souple », « proprement canadienne », est plus adaptée à l'usage que les approches plus « bureaucratiques » en Europe. Elle ne l'est pas.

Il y a vingt ans, la Commission européenne a jugé que le Canada offrait un « niveau de protection adéquat », du moins pour les entreprises visées par la LPRPDE, permettant ainsi que des données personnelles soient transmises au Canada sans qu'aucune autre mesure de protection ne soit nécessaire. Le seuil a aujourd'hui changé à la suite de jugements de tribunaux européens. L'« équivalence substantielle » à la législation européenne sur la protection des données est désormais le test d'adéquation – et elle se situe à un seuil plus élevé que lorsque la LPRPDE était jugée adéquate, il y a 20 ans. Il est d'une importance capitale pour les entreprises canadiennes que le jugement sur le caractère adéquat ne soit pas annulé. Au-delà des avantages économiques, le caractère adéquat revêt une importance symbolique, ce qui fait du Canada un endroit où les droits en matière de vie privée

[7] Le gouvernement britannique a récemment utilisé ce discours dans le cadre de son projet de loi sur la protection des données et de l'information numérique (nº 2) (*Data Protection and Digital Information ou* le « **DPDI** »). Cela dit, le DPDI est une version pratiquement inchangée du projet de loi initial annoncé en juillet 2022, qui avait été rédigé en collaboration avec des groupes représentant l'industrie et des entreprises, des groupes de défense de la vie privée et des organismes de protection des consommateurs. Bien que le DPDI et la possibilité qu'il soit jugé « adéquat » aux termes du RGPD aient fait l'objet de maints débats, le fait est qu'il ne comporte pas d'écarts importants par rapport au cadre actuel du RGPD et qu'il s'agit simplement d'une version allégée de ce dernier. Le DPDI a été présenté en grande pompe, mais ce projet de loi indique clairement que le gouvernement britannique est conscient du risque de perdre son statut d'équivalence s'il s'écarte trop du cadre établi par le RGPD, une décision qui entraînerait de grandes perturbations et qui serait préjudiciable pour nombre d'entreprises au Royaume-Uni.

continuent d'être respectés. De plus, les entreprises mondiales affirment déjà que leurs activités sont conformes au RGPD et cohérentes avec lui – y compris de nombreuses entreprises canadiennes. Alors, pourquoi y aurait-il des divergences inutiles entre le RGPD et le projet de loi C-27? Nous pourrions nous retrouver dans une situation où les entreprises accordent plus de droits aux Européens et protègent davantage les données européennes que les données canadiennes. La cohérence avec le RGPD est donc importante pour l'interopérabilité mondiale des normes de protection des données et la compétitivité des sociétés canadiennes.

Le CDN croit savoir que les fonctionnaires canadiens sont susceptibles d'avoir reçu l'assurance, en privé, de ce que le projet de loi C-27 satisfait à la norme d'« équivalence essentielle ». Le Canada ne devrait pas être aussi confiant. On note dans le présent rapport plusieurs dispositions du projet de loi C-27 qui sont considérablement plus faibles que le RGPD et qui accordent aux Canadiens des droits à la protection de la vie privée nettement inférieurs à ceux des Européens. Bon nombre des recommandations du CDN dans le cadre de l'étude du projet de loi C-27 amélioreraient considérablement la probabilité que le Canada atteigne l'équivalence essentielle. Le jugement sur l'équivalence essentielle, en vertu de l'article 45 du RGPD, est formel et fait intervenir la Commission, le Comité européen de la protection des données, les représentants des pays de l'Union européenne et, éventuellement, le Parlement européen. Les décisions concernant l'équivalence substantielle peuvent également être contestées devant les tribunaux européens. Le Canada ne devrait pas présumer que notre statut sera maintenu simplement parce que nous l'avons déjà obtenu avec la LPRPDE. Pour les raisons exposées ci-dessous, l'équivalence substantielle du projet de loi C-27 par rapport à ces normes européennes est fortement discutable.

Dans le mémoire sur le projet de loi C-27 présenté par le CPVP au *Comité permanent de l'industrie et de la technologie de la Chambre des communes* (« **INDU** ») (mai 2023), Philippe Dufresne, commissaire à la protection de la vie privée du Canada, estime que ce texte est un « pas dans la bonne direction », en ajoutant toutefois qu'il « peut et doit être amélioré davantage ». Le mémoire du CPVP contient 15 recommandations clés assorties de suggestions de modifications à apporter au projet de loi C-27, ainsi qu'une annexe où sont énumérées d'autres façons d'améliorer ce texte qui s'appuient sur les recommandations antérieures du CPVP au sujet de l'ancien projet de loi C-11. Les recommandations du CPVP sont les suivantes : reconnaître le droit à la vie privée comme un droit fondamental, protéger la vie privée des enfants, élargir la liste des violations donnant lieu à des SAP, renforcer le cadre pour les renseignements dépersonnalisés et anonymes, exiger des organisations qu'elles expliquent sur demande toutes les prévisions, les décisions et le profilage à l'aide de systèmes de décision automatisés, effectuer des EFVP pour les initiatives à haut risque, étendre la capacité du CPVP à coordonner avec d'autres organismes, réaliser des EFVP pour les initiatives à haut risque, limiter l'exception au droit à l'élimination concernant le calendrier de conservation des dossiers d'une organisation et assurer une flexibilité accrue dans l'utilisation des accords de conformité volontaire. Ces recommandations correspondent étroitement à celles présentées dans le présent rapport.

2. Présenter correctement les objectifs du projet de loi C-27

Contrairement aux lois sur la protection des renseignements personnels dans le secteur privé de nombreux autres pays, le projet de loi C-27 ne reconnaît pas le droit à la protection de la vie privée comme un droit fondamental de la personne. Il est tout à fait inapproprié d'établir un équilibre entre une perte de vie privée et la possibilité d'avantages commerciaux. Le CDN recommande de :

2.1 Reconnaître la protection de la vie privée comme un droit fondamental de la personne.

La LPVPC devrait expressément reconnaître la protection de la vie privée comme un droit humain fondamental qui est inextricablement lié à d'autres droits et libertés fondamentaux, y compris les droits à la vie et à la liberté (autonomie personnelle et autodétermination), la liberté de pensée et d'expression, la protection contre la discrimination et la protection contre les intrusions ou la surveillance injustifiées. Une telle reconnaissance devrait être faite à la fois dans un nouveau préambule de la LPRPC elle-même (à noter que le préambule actuel qui sans doute ne s'applique qu'à l'ensemble du projet de loi C-27, ne contient pas une telle reconnaissance) et dans l'article 5 « Objet » de la LPRPC afin de fournir une orientation claire à ceux et celles qui interprètent la LPVPC. L'ajout d'un renvoi à la protection de la vie privée comme étant un droit fondamental de la personne dans le préambule de la LPVPC à lui seul ne suffit pas; pour éviter tout doute, une inclusion précise est nécessaire dans le corps de la LPVPC pour donner un effet juridique non équivoque à l'intention du législateur que la protection de la vie privée soit reconnue comme un droit fondamental de la personne. Comme dans le RGPD, les droits à la vie privée des particuliers devraient l'emporter sur les intérêts commerciaux et ne pas être « mis en balance » avec ceux-ci. Toutefois, toute perte de vie privée doit être soupesée en fonction d'autres droits fondamentaux, comme le droit à la liberté d'expression. Un droit fondamental à la vie privée concerne le droit de contrôler les RP d'une personne et leur traitement, et leur traitement particulier dans le contexte du système décisionnel automatisé (**SDA**)/intelligence artificielle (**IA**), où les risques pour les droits fondamentaux (comme le droit d'être à l'abri de la discrimination et des décisions arbitraires) sont accrus. Le Commissariat à la vie privée du Canada (CVPC) a publié une opinion d'Addario Law Group S.E.N.C.R.L., s.r.l., le 31 mars 2022, selon laquelle une approche fondée sur les droits de la personne en matière de protection des données est constitutionnelle.

La décision dans l'affaire *Canada (Commissaire à la protection de la vie privée)* c. *Facebook, Inc.*, 2023 CF 533 rendue le 13 avril 2023 par la Cour fédérale du Canada illustre également la nécessité d'un cadre juridique relatif aux droits de la personne dans la législation sur la protection des renseignements personnels. Elle renvoie à la disposition de mise en balance de la LPRPDE, qui traite de la nécessité d'équilibrer les intérêts individuels et organisationnels. Toutefois, comme le montrent des cas comme le scandale Cambridge Analytica, les renseignements personnels utilisés de manière illégale peuvent conduire au profilage et au

microciblage avec des données erronées à des fins politiques. Le droit à la vie privée ne devrait pas être « échangé » contre les désirs et les intérêts des organisations. Il devrait être reconnu comme un droit fondamental de la personne, permettant à une personne d'avoir plus de contrôle sur sa vie privée et ses renseignements personnels. Toute mise en balance devrait être effectuée du point de vue de la protection de la vie privée en tant que droit fondamental de la personne.

2.2 **Modifier le nom de la loi proposée, qui passe de « *Loi sur la protection des renseignements personnels des consommateurs* » (LPRPC) à « *Loi sur la protection des renseignements personnels au Canada* » (LPRPC) ou à « *Loi canadienne sur la protection des renseignements personnels* » (LPRPC).**

Remplacer « consommateur » par « Canada » reflète mieux la portée prévue de la loi, à savoir protéger, dans le contexte des activités commerciales des organisations du secteur privé du Canada, les RP de tous les Canadiens, pas seulement ceux qui agissent en tant que « consommateurs ».

2.3 **Consulter les peuples autochtones pour moderniser la législation canadienne sur la protection des renseignements personnels.**

Le Citizen Lab de l'Université de Toronto a dénoncé le fait que le gouvernement fédéral n'a pas consulté les peuples autochtones au sujet de la modernisation de la LPRPDE dans une analyse critique du projet de loi C-27 intitulé *Minding Your Business*, publié le 22 novembre 2022 (*voir en particulier les pages 37, 38 et 54*). Les professeurs Lisa Austin et John Borrows, de l'Université de Toronto, font valoir le même argument dans leur commentaire du 6 décembre 2022 intitulé *The Digital Charter Implementation Act Ignores Indigenous Data Sovereignty*. Cette faute est contraire à l'obligation du gouvernement fédéral de mettre en œuvre la *Déclaration des Nations Unies sur les droits des peuples autochtones* (**DNUDPA**). Il est inacceptable et inexcusable, surtout à la lumière des principes bien établis et bien connus de PCAP® des Premières Nations (c.-à-d. la propriété, le contrôle, l'accès et la possession) qui ont été énoncés pour la première fois en 1998. Ces principes affirment que les Premières Nations ont le contrôle sur les processus de collecte des données et qu'elles possèdent et contrôlent la manière dont ces renseignements peuvent être utilisés.

Autrement dit, les voix autochtones ne doivent pas être laissées de côté si le gouvernement fédéral veut sérieusement établir une base de confiance dans le monde numérique au Canada. Par conséquent, le gouvernement fédéral doit au moins commencer à consulter l'Assemblée des Premières Nations (**APN**) ainsi que l'organisation technique experte, le Centre de gouvernance de l'information des Premières Nations (**CGIPN**) et surtout, les détenteurs de droits eux-mêmes. En outre, le gouvernement fédéral doit fournir à ces parties prenantes autochtones des délais et des moyens appropriés pour leur permettre de participer de manière constructive à ces consultations. Le CDN comprend, après avoir communiqué récemment avec l'APN et le CGIPN, que ce dernier a publié plusieurs ressources pertinentes en ce qui concerne la modernisation de la loi canadienne sur la

protection des renseignements personnels, notamment un document de réflexion publié en août 2022 intitulé *Exploration of the Impact of Canada's Information Management Regime on First Nations Data Sovereignty* et, plus récemment, un autre document de réflexion publié en mars 2023 intitulé *PIPEDA and First Nations: Application and Reform*.

3. Aborder la question des risques pour la démocratie liés à la protection de la vie privée

*Les scandales récents ont démontré sans équivoque comment le traitement des RP par les partis politiques et d'autres acteurs peut avoir des conséquences néfastes pour les institutions démocratiques. Il est donc tout à fait injustifiable que les partis politiques fédéraux (**PPF**) du Canada ne soient pas expressément assujettis à la LPVPC.*

3.1 Étendre expressément la LPVPC pour couvrir les partis politiques fédéraux (PPF) du Canada.

C'est le comble du cynisme et de l'hypocrisie que les PPF continuent de faire fi des recommandations des commissaires à la protection de la vie privée au Canada et à l'étranger, du Bureau du directeur général des élections du Canada, du comité ETHI, des experts en matière de protection de la vie privée et de gouvernance des données, des défenseurs et des sondages d'opinion publique visant à inclure expressément les PPF dans la loi fédérale sur la protection de la vie privée du secteur privé puis de demander à toutes les autres organisations de suivre des règles que les PPF refusent de suivre eux-mêmes. Il est peu probable que cette prétendue exclusion soit jugée « adéquate » en vertu du RGPD, particulièrement pour un Canadien vivant dans l'UE, parce qu'elle violerait l'interdiction (à quelques exceptions près) de « traitement de données personnelles révélant […] des opinions politiques » prévue au paragraphe 9 (1) du RGPD.

Cette étendue expresse peut être accomplie en 1) ajoutant au paragraphe 6 (1) de la LPVPC, un nouvel alinéa c) qui se lit comme suit : « c) qui est recueilli, utilisé ou divulgué par un parti politique fédéral, un candidat, une association de circonscription électorale ou un candidat à l'investiture dans le cadre d'activités électorales »; et 2) ajouter les définitions appropriées de « parti politique fédéral », « candidat », « association de circonscription électorale » et « candidat à l'investiture » au sens de la *Loi électorale du Canada*, et de « activités électorales » pour englober toutes les activités liées à promouvoir un parti politique fédéral à tout moment, c'est-à-dire pendant une période électorale officielle ou autrement.

Il convient de noter qu'en Colombie-Britannique, le Commissariat à l'information et à la protection de la vie privée a récemment conclu que les PPF sont assujettis à la loi sur la protection des renseignements personnels de la Colombie-Britannique. En résumé, la LPVPC peut et doit s'appliquer aux partis politiques fédéraux. La généralisation de son application serait une mesure simple et réalisable dès à présent. En outre, le gouvernement australien, dans son *Privacy Act Review Report 2022* du ministère du procureur général, publié le 16 février 2023, recommande que les partis politiques enregistrés en Australie soient assujettis à la

même loi sur la protection des renseignements personnels dans le secteur privé qui régit l'ensemble des organismes du secteur privé.

La modification apportée par le gouvernement fédéral à la *Loi électorale du Canada*, qui a reçu la sanction royale le 22 juin 2023, censée prévoir un régime national, uniforme, exclusif et exhaustif en ce qui concerne la collecte, l'utilisation et la communication par les PPF des renseignements personnels des Canadiens, d'une manière qui prétend avoir préséance sur toutes les lois provinciales en matière de protection des renseignements personnels, est non seulement hypocrite, mais elle enfreindrait la Constitution du Canada et la Charte, et elle devrait scandaliser les Canadiens pour les raisons résumées à l'annexe G.

4. Reconnaître les risques sérieux en matière de protection de la vie privée tant pour les groupes que pour les personnes

Il y a de sérieux risques pour sa vie privée chaque fois qu'une personne fait l'objet d'une classification, d'un tri ou qu'elle est « profilée » en fonction de ses RP. Ces risques peuvent être accrus lorsque la personne concernée est un groupe. Par conséquent, la réforme du droit relatif à la protection de la vie privée devrait reconnaître les risques pour les groupes, ainsi que pour les personnes, et y répondre. Plusieurs amendements permettront d'atteindre cet objectif.

4.1 Étendre la protection de la vie privée pour atténuer les risques pour les groupes.

La LPVPC devrait, pour tous les Canadiens, étendre la protection aux renseignements qui seraient considérés comme personnels à des groupes suffisamment définis, comme les ménages et les enfants dans une salle de classe. Tout comme les personnes, les groupes peuvent aussi être suivis, profilés et ciblés et cela peut avoir une incidence sur les groupes et les personnes au sein de ces groupes.

4.2 Définir les « renseignements sensibles » conformément au principe général de la sensibilité énoncé à l'article 12 de la *Loi 25* du Québec et aux catégories spéciales de renseignements personnels (RP) sensibles énumérées à l'article 9 du RGPD (pour assurer le caractère adéquat), mais sur une base non exhaustive et avec l'ajout de renseignements permettant la localisation.

À l'heure actuelle, la définition des catégories de renseignements personnels sensibles est laissée ouverte et les mots « sensible » et « sensibilité » sont utilisés dans le projet de loi C-27 sans être définis (à l'exception des mineurs). Ainsi, la définition est laissée à l'organisation avec le risque évident que certaines données sensibles ne soient pas considérées comme telles et que les interprétations varient.

Afin d'offrir une plus grande certitude aux Canadiens et aux entreprises canadiennes, et de s'aligner à la fois sur la *Loi 25* du Québec et sur le RGPD, le projet de loi C-27 devrait d'abord définir les « renseignements sensibles » en établissant un principe général de sensibilité suivi d'une liste explicitement ouverte

d'exemples (y compris les renseignements de localisation et les catégories particulières de données personnelles sensibles énumérées à l'article 9 du RGPD, à savoir les RP révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la génétique, la biométrie, la santé, la vie sexuelle ou l'orientation sexuelle).

Par conséquent, dans la même veine que celle suggérée par le CPVP dans son mémoire de mai 2021 concernant l'ancien projet de loi C-11, cette définition pourrait se lire comme suit :

> « **renseignements sensibles** » désigne les renseignements personnels pour lesquels une personne a des attentes accrues en matière de protection de la vie privée, ou pour lesquelles la collecte, l'utilisation ou la divulgation crée un risque accru de préjudice pour la personne et comprend : a) des renseignements révélant l'origine raciale ou ethnique, l'identité de genre, la vie sexuelle, l'orientation sexuelle, les opinions politiques, l'appartenance à un groupe ou les croyances religieuses ou philosophiques; b) des renseignements génétiques; c) des renseignements biométriques; d) des renseignements financiers; e) des renseignements sur la santé; et f) des renseignements de localisation.

4.3 Protéger les mineurs au moyen d'exigences de confidentialité spéciales et renforcées.

Il existe un large consensus selon lequel Internet n'a pas été conçu en pensant aux mineurs. Cela dit, la LPVPC ne répond aux besoins des mineurs en matière de protection des renseignements personnels qu'en qualifiant leurs RP de « sensibles », mais elle ne contient aucune mesure qui limite les pratiques courantes de surveillance en ligne et de manipulation du comportement des entreprises ou qui réduit même la motivation des entreprises à suivre les mineurs. La LPVPC devrait promouvoir des protections spécifiques pour les enfants et les jeunes, comme la définition de règles de consentement adaptées à l'âge, l'établissement de mécanismes et de processus respectueux de la vie privée pour la vérification de l'âge, et la fourniture d'un code de pratique complet pour les organisations qui collectent, utilisent ou divulguent les renseignements personnels des enfants (comme le *Children'*s *Code* de septembre 2020 du Royaume-Uni, en vigueur depuis 2021, et le *California Age-Appropriate Design Code Act* de septembre 2022, qui entre en vigueur le 1er juillet 2024). Il convient de noter que de telles mesures de protection des mineurs prolifèrent dans le monde entier, notamment en Irlande, aux Pays-Bas et en Argentine. Aux États-Unis, de nombreuses lois visant à renforcer la protection des renseignements personnels des enfants ou l'utilisation des médias sociaux par les mineurs ont été adoptées ou proposées, notamment dans l'Utah, le Connecticut, l'Ohio, l'Arkansas, l'Oregon, l'Illinois, le Maryland, le Nevada, le Nouveau-Mexique, le Texas, la Californie, la Floride, l'Iowa, la Louisiane, le Maryland, le Minnesota, la Caroline du Sud et le New Jersey.

Ici, au Canada, en avril 2023, le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique a publié un rapport indiquant qu'il en est aux premières étapes de l'élaboration d'un code visant à clarifier les obligations des organisations à l'égard des renseignements personnels des mineurs en vertu de la loi de la Colombie-Britannique sur la protection des renseignements personnels. La Commission d'accès à l'information (CAI) du Québec, dans son rapport au ministre responsable de l'accès à l'information et de la protection des renseignements personnels, a également suggéré que la loi 25 soit renforcée afin d'améliorer la protection de la vie privée des enfants[8].

Tout code relatif aux mineurs proposé en vertu de la LPVPC devrait tenir compte de l'intérêt supérieur du mineur en tant que préoccupation principale et exiger, entre autres, (1) la réalisation d'évaluations des facteurs relatifs à la vie privée (EFVP) afin d'atténuer le risque pour les mineurs découlant de la collecte, de l'utilisation ou de la divulgation de leurs renseignements personnels, (2) l'utilisation de paramètres de confidentialité élevés par défaut, (3) des contrôles parentaux adaptés à l'âge et (4) des outils adaptés à l'âge pour signaler les préoccupations. Conformément aux nouvelles normes internationales, un tel code devrait également interdire aux organisations de recueillir des renseignements relatifs à l'emplacement précis d'un mineur, d'utiliser des techniques dites de « coup de pouce » (même si elles ne sont pas considérées comme des interfaces truquées trompeuses) et de communiquer des données sur les mineurs à des tiers, à moins qu'il n'existe une raison impérieuse de le faire et que cela soit dans l'intérêt du mineur.

4.4 **Énoncer clairement que certaines zones où il est interdit d'aller représentent toujours des fins inappropriées pour la collecte, l'utilisation et/ou la communication des RP d'une personne.**

Ces objectifs et interdictions inappropriés devraient inclure (1) le microprofilage psychographique et le microciblage à des fins de persuasion ou d'influence sur le comportement et (2) la capture de données biométriques sans consentement exprès (par exemple, le grattage d'images faciales à partir de sites Web, de plateformes et d'autres emplacements sur l'Internet).

5. **Corriger les dispositions relatives au consentement.**

Les exigences relatives au consentement exprès et implicite, et leur lien avec l'exception de « l'intérêt légitime » continuent de créer de la confusion pour les Canadiens et les entreprises, et mettent donc en péril le statut « adéquat » continu du Canada. Par conséquent, la LPVPC devrait être révisée pour :

[8] *Mieux protéger les renseignements personnels des jeunes à l'ère* numérique; Commission d'accès à l'information, août 2022.

5.1 Renforcer le consentement valide prévu à l'article 15 de la LPVPC en rétablissant l'exigence de « compréhension » prévue à l'article 6.1 de la LPRPDE.

En 2015, l'exigence relative à la « compréhension » a été ajoutée à la LPRPDE (à l'article 6.1) comme étant la clé de la validité du consentement et pour s'assurer que le consentement est éclairé et valable. Malheureusement, cette exigence est inexplicablement absente de la Loi. Elle est remplacée par une exigence moindre selon laquelle les renseignements fournis aux personnes pour obtenir leur consentement doivent être « en langage simple qu'une personne à qui les activités de l'organisation sont destinées devrait raisonnablement comprendre ». Sans le maintien de l'exigence selon laquelle les Canadiens doivent être susceptibles de comprendre ce à quoi on leur demande de consentir, la LPVPC n'atteint pas son objectif de donner aux Canadiens un plus grand contrôle sur leurs renseignements personnels. Cela leur en donne moins. Il est possible de remédier à cette lacune en rétablissant le libellé suivant de l'article 6.1 de la LPRPDE à l'article 15 de la LPVPC (p. ex. voir l'ajout proposé au paragraphe 15(3) à la page 20 ci-dessous) :

> Le consentement d'une personne n'est valide que s'il est raisonnable de s'attendre à ce qu'une personne visée par les activités de l'organisation comprenne la nature, l'objet, et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquels elle consent.

Les commentaires troublants du juge Manson dans la décision relative à l'application Facebook, qui fait actuellement l'objet d'un appel, soulignent l'importance de cette recommandation (que le consentement valable soit renforcé en rétablissant l'exigence de « compréhension » de la LPRPDE)[9]. Plus précisément, le juge Manson cherche à s'appuyer sur des preuves subjectives concernant les attentes des utilisateurs en matière de protection des renseignements personnels « pour mieux évaluer le caractère raisonnable d'un consentement valable » qui, selon lui, peut être « particulièrement tributaire du contexte et en constante évolution ».

Les commentaires du juge Manson sont problématiques du point de vue de la protection future des renseignements personnels des Canadiens. Une telle interprétation irait à l'encontre de l'approche normative établie depuis longtemps par les tribunaux.

Comme le souligne la professeure Scassa dans son récent blogue[10], l'arrêt *R.* c. *Tessling* rendu en 2004 par la Cour suprême du Canada, selon lequel les

[9] *Le Commissaire à la protection de la vie privée porte en appel la décision de la Cour fédérale concernant l'enquête sur Facebook*, Commissariat à la protection de la vie privée du Canada, en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2023/an_230512-2/

[10] Annexe I, Bibliographie annoté, l'article 48.

attentes subjectives en matière de vie privée ne devraient pas servir à miner les protections, a établi l'approche normative applicable aux lois canadiennes en matière de protection de la vie privée. La professeure Scassa fait remarquer qu'il est de plus en plus naïf de « s'attendre raisonnablement » à une forme quelconque de protection de la vie privée dans une société grande consommatrice de données et axée sur la surveillance dont les lois sur la protection des renseignements personnels manquent de mordant.

Les commentaires du juge Manson soulignent l'importance de ne pas affaiblir davantage les dispositions de la LPRPDE relatives au consentement valable. Le projet de loi C-27 devrait plutôt préciser très clairement que le consentement valable exige qu'il soit « raisonnable de s'attendre », non pas subjectivement, mais objectivement, à ce que les individus comprennent la nature, les fins et les conséquences de la collecte, de l'utilisation et de la communication des renseignements personnels auxquels ils ont consenti.

5.2 **Adopter une règle relative aux « intérêts légitimes » qui place clairement les intérêts et les droits fondamentaux de la personne au-dessus des intérêts commerciaux de l'organisation dans toute évaluation de l'incidence de l'application de la règle.**

L'exception proposée par la LCVPC concernant l'exception des « intérêts légitimes » au consentement devrait être reformulée comme une solution de rechange légitime au consentement, plutôt qu'une exception, à condition que, dans l'évaluation des ÉFRV qui doit être effectuée par l'organisation, les intérêts et les droits fondamentaux d'une personne ne l'emportent pas sur les intérêts commerciaux de l'organisation dans la collecte ou l'utilisation des RP pertinents. Cette règle d'évaluation remplacerait la règle proposée dans le projet de loi C-27, qui prévoit un équilibre entre les intérêts commerciaux et tout effet préjudiciable potentiel sur la personne. Des exigences de transparence devraient être incluses pour la collecte et l'utilisation légales des renseignements personnels sans consentement.

Cette règle des « intérêts légitimes » suivrait la règle analogue du RGPD des « intérêts légitimes », qui est toujours assujettie à l'exception selon laquelle les « intérêts ou droits et libertés fondamentaux » de la personne l'emportent sur les fins pour lesquelles une organisation recueille, utilise ou communique les renseignements personnels d'une personne.

5.3 **Éliminer le consentement implicite comme solution de rechange au consentement exprès pour la collecte, l'utilisation ou la communication autorisées de renseignements personnels.**

Lorsqu'une justification fondée sur un « intérêt légitime » est incluse, il n'est pas nécessaire d'obtenir un « consentement implicite » comme le prévoit actuellement

le par. 15 (5) (types de consentement). Il ne devrait y avoir qu'un type de consentement, soit le consentement explicite. Si une organisation ne peut obtenir un consentement exprès, elle peut alors invoquer des intérêts légitimes. Les organisations ne devraient pas avoir le beurre et l'argent du beurre. L'exception du « consentement tacite » au consentement exprès prévue dans la LPVPC proposée devrait être éliminée. Tel qu'il est actuellement stipulé, le fondement du consentement implicite pourrait entrer en conflit avec l'exception relative aux intérêts légitimes en prévoyant un autre fondement pour le traitement autorisé des RP « en tenant compte des attentes raisonnables de la personne », mais sans les garde-fous pour assurer un niveau de protection adéquat de la vie privée, comme les exigences des ÉFRV de cette règle. Comme le prévoit le projet de loi C-27, une organisation peut faire valoir qu'elle a obtenu un consentement implicite pour le traitement de cette demande sans avoir besoin de la divulgation complète requise pour obtenir un consentement exprès ou sans satisfaire aux exigences de la règle des intérêts légitimes, même si ce traitement devrait être traité de façon plus appropriée par cette règle.

5.4 Exiger un consentement explicite et distinct sur les médias numériques[11] pour la collecte, l'utilisation ou la communication de renseignements personnels à des fins autres que celles qui sont nécessaires pour fournir un produit ou un service.

Lorsque des médias numériques désirent recueillir des renseignements personnels au-delà de ce qui est nécessaire pour fournir un produit ou un service, cette collecte devrait faire l'objet d'un consentement explicite et distinct de tout consentement donné relativement au produit ou au service en question. En outre, la personne doit pouvoir retirer son consentement à tout moment sans incidence sur la réception du service. Une telle disposition ferait en sorte que le consentement à la collecte de renseignements personnels à des fins de ciblage publicitaire ne puisse pas être dissimulé dans les conditions d'utilisation ou la politique de confidentialité du service, mais qu'il doive être porté à l'attention de la personne et obtenu par une action positive distincte de la part de cette personne.

La disposition proposée vise à tenir compte de l'évolution de la norme sur la collecte de données en ligne énoncée dans les décisions *Meta Ireland* rendues par le Comité européen de la protection des données le 5 décembre 2022 et l'Irish Data Protection Commission le 31 décembre 2022, ainsi que dans le rapport de conclusions du CPVP du 26 janvier 2023 intitulé *Enquête sur la conformité de Home Depot du Canada inc. à la LPRPDE.* Dans les cas, les attentes raisonnables de l'utilisateur étaient un facteur clé, de même que le facteur des « fins secondaires »[12].

[11] La LPVPC devrait définir le terme « médias numériques » de façon large afin d'inclure Internet, les appareils mobiles, le métavers, la réalité virtuelle et d'autres médias de communication numériques.
[12] Voir aussi la Loi 25 du Québec, par. 8.1, qui exige en fait le consentement volontaire pour la collecte de données en ligne aux fins de suivi et de profilage.

5.5 **Préciser que la norme appropriée pour déterminer l'impression générale de la personne moyenne lorsqu'il s'agit de déterminer si son consentement a été obtenu « de façon trompeuse » (et est donc invalide) est celle de la personne crédule et inexpérimentée par opposition à celle de la personne raisonnable.**

Il est important, tant pour les Canadiens que pour les organisations, que la LPVPC précise clairement que toutes les personnes, y compris celles qui sont moins averties ou expérimentées et, par conséquent, plus vulnérables, soient protégées contre les pratiques trompeuses en matière de protection des renseignements personnels. Les personnes ne devraient pas être incitées frauduleusement à consentir à la collecte, à l'utilisation ou à la divulgation de leurs renseignements personnels par des organisations qui ne sont pas honnêtes. Les « schémas de conception trompeurs » (aussi appelés « schémas obscurs ») sont des techniques d'interface trompeuses pour les mécanismes de consentement de participation (« opt-in ») et de renonciation (« opt-out ») en matière de protection de la vie privée qui sont de plus en plus utilisés par des organismes sans scrupules pour amener des personnes à donner des consentements à l'égard de leurs renseignements personnels alors qu'elles n'avaient pas l'intention de le donner. Pour déterminer si une demande de consentement ou une autre pratique de protection de la vie privée est trompeuse, la LPVPC devrait adopter le critère de la personne crédule et inexpérimentée (par opposition au critère de la personne raisonnable) établi en 2012 par la Cour suprême du Canada (CSC) dans l'affaire Richard c. Time, qui portait sur le critère de la commercialisation trompeuse en vertu de la Loi sur la protection du consommateur du Québec. Plus particulièrement, comme l'a soutenu la CSC, la personne crédule et inexpérimentée est une personne qui fait confiance, qui est pressée, et qui n'est ni prudente ni diligente. Étant donné l'interaction importante et complexe entre la législation sur la protection des renseignements personnels et la législation sur la concurrence, la norme appropriée pour la personne moyenne en ce qui concerne les « pratiques trompeuses » devrait être la même en vertu des deux lois. À cet égard, il convient de noter que le Bureau de la concurrence, dans son mémoire présenté le 15 mars 2023 à ISDE pour la modernisation de la Loi sur la concurrence, fait cette recommandation concernant la norme appropriée pour les pratiques commerciales trompeuses (voir la recommandation 4.1 dans le mémoire du Bureau).

5.6 **Pour répondre aux préoccupations concernant les dispositions relatives au consentement soulevées dans les recommandations 5.1 à 5.5 ci-dessus, les articles 15, 16 et 18 de la LPVPC devraient faire l'objet d'une révision.**

Le CDN suggère la révision suivante (une comparaison suit la version définitive ci-dessous).

Consentement

Consentement requis

15 (1) Sauf disposition contraire de la présente loi, l'organisation qui recueille, utilise ou communique des renseignements personnels doit d'abord obtenir le consentement valide de l'individu concerné.

Moment du consentement

(2) Le consentement valide doit être obtenu au plus tard au moment de recueillir les renseignements personnels ou, s'agissant de renseignements qui seront utilisés ou communiqués à des fins autres que celles qu'elle a établies et consignées en application du paragraphe 12(3), avant de les utiliser ou de les communiquer à ces autres fins.

Renseignements pour un consentement valide

(3) Le consentement n'est valide que si l'organisation fournit d'abord à l'individu concerné les renseignements suivants :

a) les fins de la collecte, de l'utilisation ou de la communication des renseignements personnels, établies par l'organisation et consignées en application des paragraphes 12(3) ou (4);

b) la manière dont les renseignements personnels seront recueillis, utilisés ou communiqués;

c) les conséquences raisonnablement prévisibles de la collecte, de l'utilisation ou de la communication des renseignements personnels;

d) le type précis de renseignements personnels que l'organisation recueillera, utilisera ou communiquera;

e) le nom des tiers ou les catégories de tiers auxquels les renseignements personnels pourraient être communiqués;

et qu'il est raisonnable de s'attendre à ce que l'individu comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la divulgation des renseignements personnels auxquelles il consent.

Langage clair

(4) L'organisation fournit les renseignements mentionnés au paragraphe (3) dans un langage clair et raisonnablement compréhensible pour un individu visé par les activités de l'organisation.

Consentement : bien ou service

(5) L'organisation ne peut, pour le motif qu'elle fournit un bien ou un service, exiger d'un individu qu'il consente à la collecte, à l'utilisation ou à la communication de renseignements personnels qui ne sont pas nécessaires à la

fourniture du bien ou à la prestation du service. L'individu qui consent à cette collecte, utilisation ou divulgation peut retirer son consentement en tout temps et l'organisation ne peut pour ce motif cesser de fournir le bien ou le service.

Consentement par médias numériques

(6) Le consentement par médias numériques à la collecte des renseignements personnels d'un individu pour des fins auxquelles il ne pouvait pas raisonnablement s'attendre doit être précis, éclairé et manifeste, donné par déclaration ou action positive claire, distincte de tout consentement exigé pour la fourniture d'un bien ou d'un service.

Consentement obtenu par tromperie

16 Il est interdit à l'organisation d'utiliser des pratiques trompeuses ou mensongères ou de fournir des informations fausses ou trompeuses pour obtenir, ou tenter d'obtenir, un consentement. La norme appropriée pour déterminer si une information est fausse ou trompeuse ou si des pratiques sont trompeuses ou mensongères est l'impression générale que l'information ou la pratique donne à la personne crédule et inexpérimentée, c'est-à-dire une personne qui fait confiance, qui se dépêche et qui n'est ni prudente ni diligente. Tout consentement ainsi obtenu n'est pas valide.

Autre fondement à la collecte et à l'utilisation des renseignements personnels

Intérêt légitime

18.1 L'organisation peut recueillir ou utiliser les renseignements personnels d'un individu si la collecte ou l'utilisation est faite en vue d'une activité dans laquelle elle a un intérêt légitime, sauf si l'emportent sur cet intérêt les intérêts ou les droits et libertés fondamentaux de l'individu qui exigent la protection de ses renseignements personnels et si, à la fois[13] :

a) une personne raisonnable s'attendrait à la collecte ou à l'utilisation en vue d'une telle activité; et

b) les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu.

Conditions préalables

18.2 Avant de se prévaloir de l'article 18.1 pour recueillir ou d'utiliser des renseignements personnels, l'organisation est tenue :

[13] Cette révision suit le libellé du RGPD.

a) de déceler tout effet négatif potentiel que la collecte ou l'utilisation est susceptible d'avoir pour l'individu;

b) de trouver et de prendre des moyens raisonnables pour réduire la probabilité que ces effets se produisent ou pour les atténuer ou les éliminer;

c) de se conformer à toute autre exigence réglementaire..

Dossier d'évaluation

18.3 L'organisation consigne son évaluation de la manière dont elle remplit les conditions visées à l'article 18.2. Sur demande du commissaire, elle lui en remet une copie.

REMARQUE : Pour faciliter la consultation, voici une comparaison des modifications (ajouts soulignés en bleu, suppressions en ~~rouge barré~~) que le CDN propose d'apporter aux versions actuelles des articles 15, 16 et 18 (concernant l'intérêt légitime) de la LPVPC.

Consentement

Consentement requis

15 (1) Sauf disposition contraire de la présente loi, les organisations doivent obtenir le consentement valide d'une personne relativement à la collecte, à l'utilisation ou à la communication de ses renseignements personnels.

Détermination du moment propice à l'obtention du consentement

(2) Le consentement de la personne doit être obtenu au plus tard au moment de la collecte des renseignements personnels ou, si les renseignements doivent être utilisés ou communiqués à une fin autre que celle déterminée et enregistrée en application du paragraphe 12(3), avant toute utilisation ou communication des renseignements à cette autre fin.

Validité du consentement

(3) Le consentement de la personne n'est valide que si, au plus tard au moment où l'organisation demande le consentement de la personne, elle lui fournit les renseignements suivants :

a) les fins auxquelles les renseignements personnels déterminés sont recueillis, utilisés ou communiqués par l'organisation et enregistrés en application des paragraphes 12(3) ou (4);

b) la façon dont les renseignements personnels seront recueillis, utilisés ou communiqués;

c) toute conséquence raisonnablement prévisible découlant de la collecte, de l'utilisation ou de la communication des renseignements personnels;

d) le type particulier de renseignements personnels qui seront recueillis, utilisés ou communiqués;

e) le nom ou les types de tiers auxquels l'organisation peut communiquer les renseignements personnels., et

S'il est raisonnable de s'attendre à ce que la personne visée comprenne la nature, l'objet et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles elle consent.

Langage simple

(4) L'organisation doit fournir les renseignements visés au paragraphe (3) dans un langage simple qu'une personne à qui les activités de l'organisation sont destinées devrait raisonnablement comprendre.

~~**Formulaire de consentement**~~

~~(5) Le consentement doit être expressément obtenu, sauf si, sous réserve du paragraphe (6), il est approprié de se fonder sur le consentement implicite d'une personne, compte tenu des attentes raisonnables de cette dernière et de la sensibilité de l'information personnellequi doit être recueillie, utilisée ou divulguée.~~

~~**Activités commerciales**~~

~~(6) Il ne convient pas de se fonder sur le consentement implicite d'une personne si ses renseignements personnels sont recueillis ou utilisés dans le cadre d'une activité visée au paragraphe 18(2) ou (3).~~

Consentement — fourniture d'un bien ou d'un service

(~~7~~5) L'organisation ne peut, à titre de condition de la fourniture d'un produit ou d'un service, exiger d'une personne qu'il consente à la collecte, à l'utilisation ou à la communication de ses renseignements personnels au-delà de ce qui est nécessaire à la fourniture du produit ou du service. Une personne peut retirer à tout moment un consentement donné à ces fins sans incidence sur la fourniture du produit ou du service.

Consentement relatif aux médias numériques

(6) Le consentement au paragraphe 5 à la collecte de renseignements personnels d'une personne obtenu relativement aux médias numériques à des fins au-delà de ce qui est nécessaire pour fournir un produit ou un service doit être exprès, éclairé et sans ambiguïté, donné par déclaration ou par une action positive claire, séparément de tout consentement requis pour la fourniture d'un produit ou d'un service.

Consentement obtenu par tromperie

16 Il est interdit à l'organisation d'utiliser des pratiques trompeuses ou mensongères ou de fournir des informations fausses ou trompeuses pour obtenir, ou tenter d'obtenir, un consentement. La norme appropriée pour déterminer si une information est fausse ou trompeuse ou si des pratiques sont trompeuses ou mensongères est l'impression générale que l'information ou la pratique donne à la personne crédule et inexpérimentée, c'est-à-dire une personne qui fait confiance, qui se dépêche et qui n'est ni prudente ni diligente. Tout consentement ainsi obtenu n'est pas valide.

Autre mode de collecte et d'utilisation

~~**Exceptions relatives à l'obligation d'obtention de consentement**~~

~~**Opérations commerciales**~~

~~**Activités commerciales**~~

~~18 (1) L'organisation peut recueillir ou utiliser les renseignements personnels d'une personne à son insu ou sans son consentement si la collecte ou l'utilisation est faite dans le cadre d'une activité commerciale visée au paragraphe (2) et que~~

~~a) qu'une personne raisonnable s'attendrait à ce que la collecte ou l'utilisation se fasse dans le cadre d'une telle activité; et~~

~~b) que les renseignements personnels ne sont pas recueillis ou utilisés dans le but d'influencer le comportement ou les décisions de la personne.~~

~~**Liste des activités**~~

~~(2) Sous réserve des dispositions réglementaires, les activités suivantes sont des activités commerciales aux fins du paragraphe (1) :~~

~~a) une activité nécessaire à la fourniture d'un produit ou d'un service que la personne a demandé à l'organisation;~~

~~b) une activité nécessaire à la sécurité de l'information, du système ou du réseau de l'organisation;~~

~~c) une activité nécessaire à sécurité d'un produit ou d'un service que la personne a demandé à l'organisation; et~~

~~d) toute autre activité prescrite.~~

Intérêt légitime

~~(3)~~18.1 Une organisation peut recueillir ou utiliser les renseignements personnels d'une personne ~~à son insu ou sans son consentement~~ si la collecte ou l'utilisation est faite dans le but d'exercer une activité dans le cadre de laquelle l'organisation a un intérêt légitime ~~qui l'emporte sur tout effet négatif potentiel sur la personne résultant de cette collecte ou de cette utilisation et~~ sauf si cet intérêt ne prime pas sur les intérêts ou les droits et libertés fondamentaux de la personne qui exigent la protection de ses renseignements personnels.et

a) qu'une personne raisonnable s'attendrait à ce que la collecte ou l'utilisation se fasse dans le cadre d'une telle activité; et

b) que les renseignements personnels ne sont pas recueillis ou utilisés dans le but d'influencer le comportement ou les décisions de la personne.

Conditions préalables

~~(4)~~18.2 Avant de recueillir ou d'utiliser des renseignements personnels en vertu ~~du paragraphe 3~~de l'article 18.1 l'organisation doit : :

a) déceler toute incidence défavorable potentielle sur la personne susceptible de résulter de la collecte ou de l'utilisation;

b) déterminer et prendre des mesures raisonnables pour réduire la probabilité que les incidences se produisent ou pour les atténuer ou les éliminer;

c) se conformer à toute exigence imposée.

Consignation d'évaluation

~~(5)~~18.3 L'organisation doit consigner son évaluation de la façon dont elle remplit les conditions énoncées au ~~paragraphe 4~~de l'article 18.2 et, sur demande, fournir un exemplaire de l'évaluation au commissaire.

Exceptions relatives à l'obligation d'obtention de consentement

Opérations commerciales

Activités commerciales
18 (1) L'organisation peut recueillir ou utiliser les renseignements personnels d'une personne à son insu ou sans son consentement si la collecte ou l'utilisation est faite dans le cadre d'une activité commerciale visée au paragraphe (2) et

(a) une personne raisonnable s'attendrait à la collecte ou à l'utilisation en vue d'une telle activité;

(b) les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu.

Liste des activités

(2) Sous réserve des dispositions réglementaires, les activités suivantes sont des activités commerciales aux fins du paragraphe (1) :

(a) une activité nécessaire à la fourniture d'un produit ou d'un service que la personne a demandé à l'organisation

(b) une activité nécessaire à la sécurité de l'information, du système ou du réseau de l'organisation;

(c) une activité nécessaire à sécurité d'un produit ou d'un service que la personne a demandé à l'organisation; et

(d) toute autre activité prescrite.

~~**Intérêt légitime**~~
~~(3) 18.1 Une organisation peut recueillir ou utiliser les renseignements personnels d'une personne à son insu ou sans son consentement si la collecte ou l'utilisation est faite dans le but d'exercer une activité dans le cadre de laquelle l'organisation a un intérêt légitime qui l'emporte sur tout effet négatif potentiel sur la personne résultant de cette collecte ou de cette utilisation et~~
~~(a) une personne raisonnable s'attendrait à la collecte ou à l'utilisation en vue d'une telle activité;~~
~~(b) les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu.~~
~~**Conditions préalables**~~
~~(4) Avant de recueillir ou d'utiliser des renseignements personnels en vertu du paragraphe (3), l'organisation doit :~~
~~(a) déceler toute incidence défavorable potentielle sur la personne susceptible de résulter de la collecte ou de l'utilisation;~~
~~(b) déterminer et prendre des mesures raisonnables pour réduire la probabilité que les incidences se produisent ou pour les atténuer ou les éliminer; et~~
~~(c) se conformer à toute exigence imposée.~~

~~**Consignation d'évaluation**~~
~~(5) L'organisation consigne son évaluation de la manière dont elle remplit les conditions visées au paragraphe (4) Sur demande du commissaire, elle lui en remet une copie.~~

6. Utiliser tous les outils de la « boîte à outils de protection de la vie privée et des consommateurs » pour promouvoir la responsabilité

Le Canada a la réputation de faire œuvre de pionnier en matière de mesures de responsabilité en matière de protection de la vie privée et de les exporter dans d'autres pays, y compris en Europe. Il est donc très étrange que certaines de ces mesures ne figurent pas dans la LPVPC. Par conséquent, plusieurs dispositions du projet de loi C-27 devraient être améliorées afin de promouvoir la responsabilité organisationnelle et de veiller à ce que la détermination du caractère adéquat soit maintenue.

6.1 **Exiger des organisations qu'elles effectuent des évaluations des facteurs relatifs à la vie privée (ÉFVP) avant l'élaboration de produits ou de services, particulièrement lorsque des technologies et des modèles d'affaires envahissants sont appliqués, lorsque des mineurs sont impliqués, lorsque des RP sensibles sont recueillis, utilisés ou divulgués et lorsque le traitement est susceptible de poser un risque élevé pour les droits et libertés des personnes.**

Les ÉFVP sont un instrument établi dans les régimes de protection de la vie privée et des données, et un élément essentiel de la preuve de responsabilité en matière de gouvernance des données personnelles. Elles sont exigées dans certaines conditions en vertu du RGPD et de la *Loi 25* du Québec. Elles sont également exigées en vertu de plusieurs lois provinciales du secteur public. Ce sont de bonnes pratiques d'affaires, et de nombreuses organisations les appliquent déjà dans le cadre de leurs programmes de gestion de protection de la vie privée. Dans le contexte de la LCVPC, elles renforceraient les dispositions relatives à la responsabilité. Elles permettraient également de s'assurer que, lorsqu'une entreprise invoque l'une des exceptions aux exigences en matière de consentement, l'entreprise a bien évalué les répercussions de ses activités sur la protection des renseignements personnels. Elles devraient être expressément exigées par la Loi.

6.2 **Exiger expressément que les organisations protègent la vie privée des personnes « dès la conception et par défaut » afin de s'aligner sur l'article 9.1 de la *Loi 25* du Québec et de l'article 25 du RGPD (pour aider à assurer le « caractère adéquat »).**

Pour ce faire, on peut ajouter à l'article 57 (1) de la LPVPC une exigence selon laquelle les mesures de sécurité d'une organisation doivent, par défaut, faire en sorte que seuls les RP d'une personne qui sont nécessaires à chaque fin précise de la collecte, de l'utilisation ou de la communication soient effectivement recueillis, utilisés ou communiqués par l'organisation. Cela est particulièrement important dans le cas des organisations qui offrent des produits ou des services technologiques au public, qui devraient (comme au Québec) être tenues d'offrir le plus haut niveau de sécurité, sans intervention de l'utilisateur.

Cette protection de la « vie privée par défaut » devrait comprendre l'élaboration et la mise en œuvre d'un cadre de gouvernance de « contrôle dès la conception » (**CdC**) qui ferait passer la gouvernance des RP des concepteurs de technologies et

de leurs pratiques d'autosurveillance aux pouvoirs démocratiquement responsables (**PDR**) permettant aux Canadiens de surveiller leurs RP. En vertu du cadre de gouvernance de CdC, les ensembles de données sur les renseignements personnels importants seraient contrôlés par des PDR responsables envers les Canadiens (tant les particuliers que les groupes). Pour de plus amples renseignements sur les raisons et la nature du CdC, veuillez voir la recommandation 11.1 de l'Annexe « B ».

6.3 Promouvoir l'élaboration de modèles d'intendance des données

La LPVPC devrait inclure une disposition qui encourage le développement de modèles d'intendance des données selon lesquels les informations, à la fois personnelles et non personnelles, peuvent être fournies à un gestionnair e de données ou à une installation (ou éventuellement à un service central de données) autorisés à mettre ces données à la disposition des parties intéressées à les utiliser, de manière protégée, à des fins désignées, notamment pour tirer parti des possibilités économiques, de a recherche, de la planification du secteur public et des avantages sociaux. Un tel modèle aurait une portée plus large que celle de la définition d'« objet bénéfique sur le plan social » à l'article 39 2) de la LPVPC (c'est-à-dire « un objet lié à la santé, à la fourniture ou à l'amélioration d'installations ou d'infrastructures publiques, à la protection de l'environnement ou à toute autre fin prescrite ») et ne serait pas limité aux entités du secteur public. Parce que les modèles de gestion des données sont encore expérimentaux, toute autorisation de ce type doit être fondée sur une ÉFPV, ne doit être accordée à l'avance que pour une période de temps limitée (renouvelable) et être soumise à un examen indépendant rétrospectif pour s'assurer que l'objectif désigné est atteint en pratique.

6.4 Renforcer les mesures de sécurité

Plus précisément, exiger des organisations qu'elles tiennent compte des conséquences potentielles, tant pour les personnes que pour la société, par le biais de mesures telles que les ÉFVP, d'une violation des mesures de sécurité en plus de prendre en compte, comme déjà énoncé à l'article 57 de la LPVPC, la sensibilité, la quantité, la distribution, le format et la méthode de stockage de l'information.

La récente décision *Facebook* contient des observations qui, comme l'a fait remarquer la professeure Teresa Scassa, « devraient tirer la sonnette d'alarme au sujet du projet de loi C-27 ». En particulier, la décision stipule que les obligations de protection des renseignements personnels prennent fin après que les renseignements personnels ont été communiqués à un tiers. Cette interprétation se fonde en partie sur l'existence de la dérogation prévue par la LPRPDE pour les opérations commerciales, en vertu de laquelle les renseignements personnels peuvent être utilisés et communiqués sans consentement dans le cadre d'une opération commerciale, à condition que les parties à l'opération concluent une entente selon laquelle la partie qui reçoit les renseignements (l'acheteur) continuera d'appliquer des obligations de protection aux renseignements personnels

communiqués. Comme l'a souligné la professeure Scassa, d'autres dispositions de protection pourraient être nécessaires dans le projet de loi C-27 pour traiter, par exemple, des renseignements personnels qui peuvent être communiqués à l'insu de la personne concernée ou sans son consentement dans certaines circonstances, notamment à des fins bénéfiques sur le plan social en vertu de l'article 39. Le projet de loi C-27 devrait exiger que les organisations qui communiquent des renseignements personnels (y compris des renseignements dépersonnalisés) sans consentement à des fins précises autorisées, comme des fins bénéfiques sur le plan social, prévoient des dispositions contractuelles pour protéger les renseignements personnels après leur communication.

6.5 **Comme la *Loi 25* du Québec, la LPVPC devrait avoir une disposition distincte pour les flux de données transfrontaliers exigeant que les organisations au Canada qui exportent des RP vers un territoire étranger aux fins de traitement doivent d'abord effectuer une ÉFVP pour établir que les RP recevront un niveau de protection équivalent à celui du Canada.**

Le projet de loi C-27 ne contient aucun article portant expressément sur la question essentielle de la circulation transfrontalière des données. Malgré les nombreuses recommandations des experts, le projet de loi C-27 continue de faire fi du fait que le contexte des transferts aux fournisseurs de services à l'échelle nationale est différent du contexte des transferts effectués à l'échelle internationale. Ce n'est pas comme si le projet de loi C-27 ne reconnaissait pas l'échange généralisé et rapide de données entre les pays. Le préambule précise que le Canada est un pays commerçant, qui dépend de l'échange de renseignements personnels et de données entre les frontières. L'omission délibérée d'un article spécifique, ou même de toute disposition pertinente de fond, pour traiter de cette question est une grave lacune du projet de loi C-27 qui pourrait être corrigée en examinant d'autres compétences comparables, y compris la *Loi 25* du Québec.

Comme au Québec, tout risque supplémentaire doit être identifié, justifié, atténué et documenté dans une EFVP. De plus, l'EFVP doit inclure une évaluation du niveau plus large de protection des droits à la vie privée et de la personne dans le pays étranger, y compris la façon dont les droits à la vie privée des Canadiens peuvent être appliqués. Si le statut d'adéquation du Canada est maintenu, il sera beaucoup plus facile pour les entreprises de préparer de telles EFVP lors de l'envoi de RP vers l'Union européenne.

6.6 **Adopter un régime plus complet régissant les tiers fournisseurs de services et de traitement de données**

La LPVPC devrait établir un régime exhaustif régissant les tiers fournisseurs de services et de traitement de données, qui prévoirait des exigences contractuelles minimales, qui imposerait directement des obligations comparables au RGPD, y compris des exigences en matière de responsabilité allant au-delà de la simple sécurité, comme le propose la LPVPC. De plus, ce régime devrait établir une distinction entre les flux de renseignements personnels entièrement à l'intérieur du

Canada et ceux du Canada vers un autre pays et prévoir des mesures de protection plus strictes pour les flux de renseignements personnels qui traversent les frontières.

6.7 **Imposer clairement des obligations de transparence et de responsabilité aux courtiers en données.**

Les courtiers en données (c'est-à-dire, les tiers qui ne sont pas des fournisseurs de services) sont un aspect largement invisible et très problématique du modèle commercial de surveillance et de l'écosystème de l'industrie AdTech. La LPVPC devrait inclure des règles particulières applicables aux courtiers en données afin de veiller à ce que ce secteur du trafic de données soit réglementé efficacement en vertu de la loi fédérale sur la protection de la vie privée dans le secteur privé. Conformément à la loi de l'Union européenne sur la gouvernance des données (applicable depuis le 1er septembre 2023), une obligation fiduciaire envers les personnes devrait être imposée sur tous les intermédiaires dans la chaîne d'approvisionnement des données afin de garantir que ces courtiers de données n'utilisent les renseignements personnels qui leur sont confiés qu'aux fins prévues par les personnes auxquelles se rapportent ces renseignements. De plus, la LPVPC devrait obliger les courtiers de données à rendre leurs rôles plus visibles en exigeant qu'ils transmettent leur identité en aval dans la chaîne d'approvisionnement des données (ou peut-être certaines exigences officielles d'inscription, par exemple sur le modèle du registre proposé à la recommandation 11.3 ci-dessous et analogues aux exigences de la proposition du *DELETE Act* des États-Unis[14]).[15] Le Parlement aurait intérêt à examiner la Loi sur la gouvernance des données de l'Union européenne et le rôle des intermédiaires de données comme modèle de rechange aux géants du numérique, où les prestataires de services d'intermédiation de données qui interviennent dans l'échange de données doivent s'inscrire

[14] En vertu de la proposition de loi fédérale américaine « *Data Elimination and Limiting Extensive Tracking and Exchange Act* » (le « DELETE Act »), chaque courtier en données inscrit qui conserve des « identifiants persistants » (comme des adresses de courriel, des numéros de téléphone, des adresses physiques) devra payer à la Federal Trade Commission un abonnement annuel déterminé par cette dernière pour accéder à la base de données du système centralisé d'effacement des données. Les frais d'abonnement choisis par la FTC ne peuvent excéder 1 % du coût annuel prévu pour le fonctionnement du système centralisé et des registres hachés, selon la décision de la FTC (sous-alinéa 2(b)(3)(B)).

[15] De même, le 14 septembre 2023, la législature californienne a adopté le Delete Act (Senate Bill 362) qui oblige tous les courtiers en données à s'inscrire auprès de la California Privacy Protection Agency (CPPA), moyennant le paiement d'un droit. Une fois ratifiée par le gouverneur, la loi californienne exigera de la CPPA qu'elle crée, d'ici au 1er janvier 2026, un « mécanisme de suppression » public par lequel un consommateur (ou un mandataire autorisé) pourra demander, en une seule fois et de manière vérifiable, à tous les courtiers en données de supprimer les renseignements personnels du consommateur. À compter du 1er août 2026, les courtiers en données devront accéder au mécanisme de suppression au moins une fois tous les 45 jours, et dans les 45 jours suivant la réception d'une demande, supprimer les renseignements personnels du consommateur (sous réserve des exemptions limitées de suppression prévues par la CPPA). Dès le 1er janvier 2028, et tous les trois ans par la suite, les courtiers en données devront faire l'objet d'une vérification par un tiers indépendant afin de s'assurer qu'ils respectent la loi. Ils seront tenus de conserver pendant au moins six ans les dossiers relatifs à toutes les vérifications de conformité et de les présenter sur demande à la CPPA. À partir du 1er janvier 2029, les courtiers en données devront dévoiler les résultats de leurs vérifications lorsqu'ils s'inscriront auprès de la CPPA.

publiquement et avoir l'obligation fiduciaire de s'assurer qu'ils agissent dans l'intérêt supérieur des personnes concernées.

7. Renforcer le contrôle des personnes sur leurs RP

Des modifications doivent être apportées au projet de loi C-27 afin que les personnes puissent transférer, supprimer et accéder efficacement à leurs données (conformément à l'objectif du Canada de maintenir son statut « adéquat »). Les Canadiens devraient également pouvoir contester les décisions prises à leur sujet par les systèmes SDA/IA et disposer d'un droit privé d'action en cas de violation de la vie privée. Par conséquent, le CDN recommande que la LPVPC comprenne ce qui suit :

7.1 Fournir un droit plus complet à la « mobilité » des RP (alias « portabilité »).

La LPVPC propose un droit accordé aux personnes uniquement dans le contexte des « cadres de mobilité des données » qui est limité à deux aspects essentiels : premièrement, les RP pouvant être transférés sont limités à ceux que l'organisation elle-même a collectés auprès de la personne; et deuxièmement, les RP de la personne sont transférés de l'organisation qui a collecté les RP à une autre organisation désignée par la personne. Une personne devrait être en mesure de recevoir ses RP directement de l'organisation afin de 1) maximiser le contrôle qu'elle exerce sur ses RP, 2) encourager la concurrence et soutenir l'innovation, et 3) s'aligner sur le RGPD (et être interopérable avec son droit à la mobilité et à la transférabilité des données en vertu de la Loi du Québec qui entrera en vigueur le 22 septembre 2024. De plus, une personne devrait également avoir le droit de transférer tout RP qu'elle a fourni à une organisation, par exemple en remplissant des formulaires en ligne ou par l'organisation en observant les activités de la personne en ligne.

7.2 Limiter les exceptions au droit au retrait » des RP (c'est-à-dire le droit de « supprimer », d'« effacer » ou d'« être oublié ») et fournir le droit au retrait en ce qui concerne « l'indexation des RP des personnes » par les moteurs de recherche dans des circonstances précises.

Le droit au retrait ne devrait pas faire l'objet d'exceptions qui limitent de façon déraisonnable la portée potentielle de la disposition, y compris l'utilisation dans le cadre de la fourniture d'un produit, de demandes raisonnables de suppression en vrac et du calendrier de conservation des dossiers d'une organisation. Le droit au retrait devrait s'appliquer aux plateformes en ligne en ce qui concerne l'indexation des RP au moyen de moteurs de recherche en ligne dans des circonstances précises, comme l'illégalité ou l'atteinte à la vie privée ou à la réputation d'une personne, sous réserve du droit du public à la liberté d'expression.

7.3 **Renforcer l'information et l'accès.**

Plus précisément, à l'article 63 de la LPVPC, rétablir le libellé et l'objet du principe 9 de la LPRPDE (c.-à-d. 4.9.3) concernant l'accès individuel comme suit :

> 4.9.3 L'organisation qui fournit le relevé des tiers à qui elle a communiqué des renseignements personnels au sujet d'une personne devrait être la plus précise possible. S'il lui est impossible de fournir une liste des organisations à qui elle a effectivement communiqué des renseignements au sujet d'une personne, l'organisation doit fournir une liste des organisations à qui elle pourrait avoir communiqué de tels renseignements.

7.4 **Interdire, sous réserve d'exceptions précises et limitées, aux organisations d'utiliser les systèmes SDA/AI, sous réserve d'exceptions limitées, pour recueillir, utiliser ou communiquer les RP d'une personne comme fondement de leurs décisions à leur sujet afin de s'aligner sur l'article 22 du RGPD (pour aider à assurer le « caractère adéquat »).**

Plus précisément, ajouter une disposition à la LPVPC accordant aux personnes le droit de ne pas être soumis à une décision fondée uniquement sur le SDA/IA qui produit des effets juridiques sur eux ou les affecte de manière aussi importante, sous réserve des exceptions suivantes : (a) la décision est nécessaire à un contrat entre la personne et l'organisation, (b) la décision est par ailleurs autorisée par la loi, ou (c) la personne a expressément consenti à la décision. De plus, la LPVPC devrait tenir compte de tout renforcement de la protection des renseignements personnels qui interdit à une organisation l'utilisation de SDA/IA en association avec des RP, comparable à ce qui a été proposé dans la *Proposition de règlement établissant des règles harmonisées en matière d'intelligence artificielle* publiée en avril 2021 (la ***loi sur l'IA* de l'UE**). Le 14 juin 2023, les ministres du Parlement européen ont adopté la loi sur l'IA de l'Union européenne comme fondement de la législation sur l'IA dans les États membres de l'Union européenne[16]. La loi sur les données d'IA de l'Union européenne interdit les systèmes ADS/AI, qui présentent un niveau de risque inacceptable, ou qui sont intrusifs ou discriminatoires. Par exemple, la *loi sur l'IA* de l'UE interdit les SDA/IA qui présentent un niveau de risque inacceptable ou qui sont intrusifs ou discriminatoires. L'interdiction vise les systèmes qui :

- font appel à des techniques subliminales ou intentionnellement manipulatrices;
- exploitent les vulnérabilités des individus, sont utilisés pour la notation sociale (comme la classification des individus en fonction de leur

[16] Voir l'article intitulé *Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle,* Parlement européen, 14 juin 2023, en ligne : https://www.europarl.europa.eu/news/fr/headlines/society/20230601STO93804/loi-sur-l-ia-de-l-ue-premiere-reglementation-de-l-intelligence-artificielle.

comportement social, de leur statut socio-économique ou de leurs caractéristiques personnelles);
- utilisent des systèmes d'identification biométrique à distance « en temps réel » dans les espaces accessibles au public, par exemple la reconnaissance faciale;
- utilisent des systèmes d'identification biométrique à distance « à posteriori », à la seule exception des forces de l'ordre pour les poursuite relatives à des crimes graves, et seulement après autorisation judiciaire;
- déploient des systèmes de catégorisation biométrique utilisant des caractéristiques sensibles (par exemple, le sexe, la race, l'appartenance ethnique, le statut de citoyenneté, la religion et l'orientation politique); des systèmes de police prédictive (fondés sur le profilage, la localisation ou le comportement criminel antérieur);
- utilisent des systèmes de reconnaissance des émotions dans les domaines de l'application de la loi, de la gestion des frontières, du lieu de travail et des établissements d'enseignement;
- font appel à la récupération sans discernement de données biométriques provenant des médias sociaux ou d'enregistrements de vidéosurveillance pour créer des bases de données de reconnaissance faciale (en violation des droits de la personne, notamment du droit au respect de la vie privée)[17].

La *loi sur l'IA* de l'UE répertorie également les domaines qui présentent un risque élevé pour la santé, la sécurité, les droits fondamentaux ou l'environnement. Il s'agit notamment de systèmes d'IA utilisés pour influencer les électeurs lors des campagnes politiques et des systèmes de recommandation utilisés par les plateformes de médias sociaux.

7.5 Donnez aux personnes le droit de contester et de s'opposer au SDA/AI qui les concerne, pas seulement un droit à la « transparence algorithmique ».

Pour ce faire, on peut inclure des dispositions précises visant à assurer l'innovation « responsable » et l'utilisation « responsable » des systèmes SDA/IA, comme : 1) un droit des personnes à une explication significative mieux articulée que l'explication énoncée à l'article 63 (3) de la LPVPC (comme « une explication qui permet aux personnes de comprendre la nature et les éléments de la décision à laquelle elles sont confrontées » ou les règles qui définissent le traitement et les principales caractéristiques de la décision ») et incluant l'obligation que l'organisation fournisse des informations sur la légitimité, l'exactitude, la fiabilité, les conséquences raisonnablement prévisibles, les risques potentiels, les mesures d'atténuation et les garanties du processus SDA/IA; 2) en tant que compléments

[17] Parlement européen, communiqué de presse : « Un pas de plus vers les premières règles sur l'intelligence artificielle », https://www.europarl.europa.eu/news/fr/press-room/20230505IPR84904/un-pas-de-plus-vers-les-premieres-regles-sur-l-intelligence-artificielle

nécessaires au droit à une explication, a) le droit des personnes d'exprimer leur point de vue à un intervenant humain et de contester la décision (que les personnes aient consenti ou que l'organisation se soit appuyée sur une exception au consentement) et b) le droit des personnes de s'opposer au consentement concernant la décision ou de le retirer, et 3) l'obligation pour les organisations utilisant l'IA de fournir la preuve de leur responsabilité (c'est-à-dire en les obligeant à consigner et à retracer leur collecte et leur utilisation des RP dans le cadre du traitement complexe effectué par leurs systèmes d'IA), et en donnant au commissaire à la protection de la vie privée le pouvoir de vérifier et d'inspecter ces registres et pratiques). Ces améliorations aux dispositions incomplètes de la LPRPC en matière d'intelligence artificielle et de SDA/AI sont décrites plus en détail dans le rapport du commissaire à la protection de la vie privée du 12 novembre 2020 intitulé *Cadre réglementaire de l'intelligence artificielle : Recommandations de réforme de la LPRPDE*.

7.6 **Renforcer le droit d'action privé (DAP).**

Cela peut être accompli en supprimant les conditions préalables à l'exercice du droit privé d'action prévu à l'article 107 de la LPVPC, à savoir que 1) le commissaire à la protection de la vie privée a conclu qu'il y a eu infraction à la LPVPC par l'organisation et cette conclusion n'a pas fait l'objet d'un appel par l'organisation, ou le Tribunal des renseignements personnels et de la protection des données (**le Tribunal**) a rejeté l'appel de l'organisation de cette conclusion, ou 2) le Tribunal a conclu que l'organisation a enfreint la LPVPC. Le temps et le coût requis pour remplir ces conditions préalables empêcheront l'accès à la justice pour la plupart des personnes visées par le DAP. Les tribunaux ont une plus grande expertise que le commissaire ou le Tribunal pour ce qui est d'entendre les témoignages et de tirer des conclusions de fait et rendre des décisions sur la responsabilité civile. Ce sont les tribunaux, et non le commissaire, qui rendront les décisions exécutoires qui élaboreront le droit de la responsabilité civile en cas de violation de la LPVPC. Par conséquent, ni le Commissaire à la protection de la vie privée ni le Tribunal ne devraient agir comme gardiens du DAP. Les réclamations frivoles ou vexatoires présentées par des particuliers ou par un groupe proposé peuvent être rejetées en vertu des règles de procédure disponibles devant les tribunaux.

L'approche la plus simple consisterait à adopter une simple disposition semblable à celle de l'article 36 de la *Loi sur la concurrence* (qui accorde un droit de recours à quiconque a subi des pertes ou des dommages par suite d'une contravention aux dispositions pénales de la Loi sans conditions préalables). La réparation en vertu de la LRPC proposée par la LPVPC se limite aux « dommages-intérêts pour perte ou préjudice subis par la personne » par suite d'une contravention. La réparation devrait être élargie pour inclure les « dommages moraux » puisque la plupart des contraventions n'entraîneront pas une perte pécuniaire pouvant être prouvée. Il faudrait également envisager de prévoir des dommages-intérêts minimaux pour les contraventions à la LPVPC. Les particuliers devraient également avoir le droit de

demander une injonction pour interdire les contraventions continues à la LPVPC. De plus, la LPVPC devrait préciser qu'il ne s'agit pas d'un « code complet » et qu'il ne doit pas être interprété comme privant quiconque d'un droit d'action civil (c'est-à-dire que les particuliers peuvent encore poursuivre les organisations pour des violations de la vie privée en common law, que ce soit en matière contractuelle, délictuelle ou autre motif juridique). Pour assurer la participation du commissaire, il peut lui être utile d'être avisé de toute action privée et d'avoir le droit d'y intervenir.

7.7 **Ajuster le régime proposé par la LPVPC pour les renseignements non identifiables afin de préciser que les organisations doivent appliquer des processus appropriés pour anonymiser et protéger ces renseignements, et ii) pour faire en sorte que les renseignements anonymisés respectent les normes énoncées dans les règlements, pour s'aligner avec la *Loi 25* du Québec.**

La définition de « anonymiser » devrait être modifiée afin de préciser que les processus appropriés prescrits par règlement doivent être mis en place pour veiller à ce qu'aucune personne ne puisse être identifiée directement à partir des renseignements. La définition devrait tenir compte du fait que les renseignements sont anonymisés s'ils sont dépouillés d'identificateurs directs conformément aux normes établies par règlement ou par l'ajout d'un renvoi précis à la définition de l'article 74. L'article 74 devrait être modifié pour exiger que des protections techniques et administratives soient appliquées à tous les renseignements anonymisés. Le régime énoncerait des exigences concernant les processus d'anonymisation ainsi que les garde-fous, y compris des obligations de transparence et de responsabilité, afin de maintenir le statut non personnel des renseignements obtenus dans les utilisations en aval. De plus, le régime doit tenir compte du fait qu'il est pratiquement impossible d'obtenir des données véritablement « anonymisées » pour quelque ensemble de données que ce soit; la définition de « renseignements anonymisés » devrait être modifiée pour refléter cette réalité, pour s'aligner avec la *Loi 25* du Québec. Le régime de réglementation doit comprendre des dispositions prévoyant des ÉFPV et un examen indépendant pour assurer la conformité.

Les modifications recommandées aux dispositions du projet de loi C-27 concernant les renseignements non identifiables sont conformes à l'**exposé du 7 décembre 2022 sur le projet de loi C-27** du Canadian Anonymization Network (**CANON**), mais vont plus loin que ce dernier en ce qui concerne les exigences en matière de protection des renseignements dépersonnalisés et anonymisés.

8. Donnez plus de mordant au commissaire à la protection de la vie privée

Le modèle du tribunal proposé dans le projet de loi C-27 est mal conçu, sans précédent, injustifié, coûteux et déroutant. Le projet de loi C-27 doit moderniser ses propositions et renforcer la structure existante de conformité et d'application de la loi du Commissariat à la protection de la vie privée du Canada.

8.1 Supprimer le Tribunal des renseignements personnels et de la protection des données proposé

La création proposée du Tribunal est mal conçue et sans justification apparente. Il ne fera qu'introduire une complexité, des délais[18] et de l'incertitude sans précédent * et inutiles pour les particuliers et les organisations dans le règlement d'une plainte. Cette complexité, ce retard et cette incertitude pourraient miner, aux yeux des gens, l'influence du commissaire à la protection de la vie privée à protéger efficacement et définitivement leur droit à la vie privée. Cela pourrait aussi miner la confiance que les organisations pourraient avoir dans le commissaire à la protection de la vie privée pour établir des règles du jeu équitables pour toutes les organisations qui se conforment à la LPVPC. Cela dit, si le Tribunal est aboli, la LPVPC doit, à la lumière des sanctions importantes et des autres ordonnances envisagées, inclure des dispositions rigoureuses en matière de procédure et de surveillance judiciaire.

Aucune justification (innovation en droit de protection de la vie privée ou autre) n'a été donnée pour le tribunal. Son rôle et sa composition soulèvent de sérieuses préoccupations (notamment une complexité, des délais et de l'incertitude inutiles pour les personnes et les organisations dans le règlement d'une plainte. De plus, aucun régime de droit en matière de protection de la vie privée au monde n'a établi un tribunal comme le Tribunal proposé en vertu de la LTPRPD (y compris les régimes modernes et progressistes de l'UE et de la Californie, ainsi que les régimes de l'Utah, du Colorado, de la Virginie et du Connecticut, et le projet de loi américain qui s'intitule *American Data Privacy and Protection Act*). Ce tribunal n'est pas non plus proposé dans le Privacy Act Review Report 2022 du 16 février 2023 du gouvernement australien.

8.2 Prévoir une application plus souple.

Bien que l'article 94 de la LPVPC stipule certains facteurs généraux qui doivent être pris en compte dans l'établissement des sanctions administratives pécuniaires **(SAP**) et des amendes, ceux-ci devraient être élargis pour inclure tous les facteurs aggravants et atténuants spécifiques et pertinents stipulés dans d'autres lois

[18] Par exemple, l'Information Commissioner's Office (ICO) du Royaume-Uni a ouvert une enquête en 2018, ce qui a donné lieu à un avis d'exécution adressé à Experian en 2020. Experian a interjeté appel de l'affaire auprès du First Tiers Tribunal du Royaume-Uni. Celle-ci a été entendue par le tribunal en 2022 et ce dernier a rendu sa décision en 2023, soit près de cinq ans après le début de l'enquête. L'affaire pourrait encore être en cours puisque l'ICO doit décider s'il interjettera appel de la décision

fédérales visant à protéger les Canadiens. (comme dans la *Loi canadienne anti-pourriel* (**LCAP**) et la *Loi sur la concurrence*). Ces facteurs pourraient comprendre la fréquence et la durée de la conduite et la vulnérabilité des personnes touchées. De plus, les facteurs d'établissement des SAP et des amendes devraient comprendre spécifiquement la sensibilité des RP dont l'organisation qui contrevient à la LPRPC est responsable. Cette souplesse permettra une application plus adaptée et plus efficace de la loi contre toutes les organisations, grandes ou petites. Il sera également plus sensible à la diversité des petites et moyennes entreprises dans l'économie canadienne.

8.3 **Doter le Commissaire à la protection de la vie privée du pouvoir de demander l'imposition de sanctions administratives pécuniaires (SAP) d'une manière semblable aux pouvoirs du Commissaire de la concurrence en vertu de la *Loi sur la concurrence*.**

Le commissaire à la protection de la vie privée doit avoir la capacité de demander aux tribunaux des montants spécifiques de SAP à l'encontre de mauvais acteurs, plutôt que de se limiter uniquement à faire des recommandations au Tribunal, (comme c'est actuellement le cas en vertu de la LPVPC). La capacité de demander des SAP est un complément naturel aux pouvoirs du commissaire à la protection de la vie privée de rendre des ordonnances de conformité de type injonction et permettra de régler certaines questions de manière plus rapide et en temps opportun. Tout comme le commissaire de la concurrence, le commissaire à la protection de la vie privée devrait pouvoir négocier clairement et expressément un paiement financier par une organisation dans le cadre d'un accord de conformité qui, à son tour, est approuvé par les tribunaux avec le consentement des deux parties.

8.4 **Habiliter le commissaire à la protection de la vie privée à émettre des « avis d'application » et élargir les dispositions pour lesquelles le commissaire à la protection de la vie privée peut recommander des sanctions afin d'inclure les violations des éléments suivants : 12 (1) (Fins appropriées); 55 (3) (Élimination à la demande d'un particulier : Refus motivé); 73 (Plaintes et demandes de renseignements); 75 (Interdiction de réidentification); et 97 (Vérifications).**

La LPVPC devrait habiliter le commissaire à la protection de la vie privée à délivrer un « avis d'exécution » à une organisation lorsqu'il est convaincu que l'organisation ne s'est pas conformée à certaines obligations fondamentales prévues par la LPVPC. Cet avis donnera à l'organisation un délai précis dans lequel elle devra se conformer (absence d'appel de l'avis), à défaut de quoi le commissaire à la protection de la vie privée pourra émettre un « avis de pénalité » imposant les exigences qu'il jugera appropriées aux fins de remédier à la non-conformité et à l'échec, y compris une SAP. Ce pouvoir pourrait s'inspirer du pouvoir d'émettre des avis d'exécution et de pénalité accordé au commissaire à l'information du Royaume-Uni (R.-U.) en vertu des articles 149, 150 et 155 de la *Data Protection Act*, 2018 du R.-U.

8.5 **Renforcer les dispositions relatives à la collaboration et à l'échange de renseignements interorganismes entre le commissaire à la protection de la vie privée, le commissaire de la concurrence et le CRTC.**

La LPVPC, la *Loi sur la concurrence* et la *Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes* devraient permettre l'échange de renseignements et la coopération entre le commissaire à la protection de la vie privée, le commissaire de la concurrence et le CRTC relativement à leurs devoirs, pouvoirs et fonctions respectifs en vertu de cette loi et pour l'administration efficace de leur législation pertinente d'une manière similaire à celle prévue par la LCAP. La loi devrait permettre la consultation des trois organismes de réglementation, y compris l'obligation de collaborer lorsqu'ils reçoivent des demandes de renseignements étrangers. Dans sa forme actuelle, la LPRPC ne permet que l'échange de renseignements et la recherche conjointe entre le commissaire à la protection de la vie privée, d'une part, et le commissaire de la concurrence, ou le CRTC, d'autre part. Les dispositions relatives à la collaboration dans la législation devraient prévoir un échange d'informations et une collaboration tripartites.

8.6 **Renforcer le régime de signalement.**

La protection de la confidentialité du divulgateur par le commissaire à la protection de la vie privée et l'interdiction pour l'employeur de prendre des mesures de représailles contre un employé dénonciateur aux articles 126 et 127, respectivement, de la LPVPC sont nécessaires, mais insuffisantes. Pour encourager les employés à signaler un comportement répréhensible, le lanceur d'alerte devrait avoir droit à une indemnité discrétionnaire fondée sur un pourcentage du total des sanctions pécuniaires recouvrées du délinquant ou des paiements volontaires faits par celui-ci. De plus, conformément à la *Directive de l'UE sur les lanceurs d'alerte*, les dispositions de la LPVPC sur les lanceurs d'alerte devraient être améliorées pour inclure 1) une limitation de la responsabilité des lanceurs d'alerte (c.-à-d., à condition qu'ils aient des motifs raisonnables de croire que le signalement était nécessaire pour révéler une infraction) et 2) un « renversement du fardeau de la preuve » sur l'organisation (c.-à-d., lorsqu'il y a des poursuites judiciaires concernant un préjudice subi par un lanceur d'alerte, il est présumé que le préjudice a été causé en relation avec le signalement. Cette inversion du fardeau de la preuve impose aux organisations la responsabilité de démontrer que toute mesure prise après le signalement n'a pas été prise à des fins de représailles.

8.7 **Mettre en place un programme d'autodéclaration pour les organisations.**

La LPVPC devrait mettre en œuvre un programme d'autodéclaration qui offre l'immunité ou un traitement indulgent aux organisations qui sont parties à des accords qui contreviennent à la LPVPC. En incitant les parties à demander l'immunité ou la clémence en échange de leur collaboration à une enquête, on améliorera la détection, l'enquête et la poursuite de telles ententes qui pourraient autrement demeurer inconnues. De plus, les programmes d'autodéclaration peuvent

accorder l'immunité ou un traitement clément aux administrateurs et aux dirigeants d'une organisation qui a été partie à une entente qui contrevient à la LPVPC, ce qui peut encourager les personnes à divulguer des renseignements et à collaborer sans craindre que leur responsabilité personnelle ou celle d'autres personnes ne leur soit imposée.

9. La *Loi sur l'intelligence artificielle et les données (LIAD)* comporte des lacunes fondamentales; elle nécessite des consultations appropriées et devrait être réexaminée (sans pour autant être confiée uniquement à ISDE).

La LIAD n'est tout simplement pas prête et doit faire l'objet de consultations appropriées pour répondre aux besoins d'aujourd'hui et de demain. La publication tardive par l'ISDE, le 13 mars 2023, de son « document d'accompagnement » visant la clarification de la LIAD, déposée par le gouvernement le 16 juin 2022, ne corrige pas ces lacunes fondamentales. Pour les raisons énoncées à l'annexe « F », le document d'accompagnement de l'ISDE ne laisse aucun doute : « Aucune LIAD n'est meilleure que la présente LIAD ».

De même, la consultation d'ISED en août et septembre 2023 sur le projet Garde-fous canadiens pour l'IA générative : un code de pratique était problématique pour les raisons énoncées dans la lettre ouverte du professeur Clement au ministre d'ISED, publiée ici.

9.1 La LIAD ne convient pas et est incomplète.

L'ajout de la LIAD au projet de loi C-27 est surprenant en raison de l'absence de consultation à son égard et de son exclusion du défunt ancien projet de loi C-11. Une bonne partie de la substance de la loi proposée est inspirée de règlements qui ne sont pas encore élaborés, ce qui force le Parlement à adopter une loi sans en comprendre la portée et l'application véritables. Cette incomplétude s'étend à des définitions cruciales dans la LIAD, comme les « systèmes à fort impact », un concept qui restreint les obligations des acteurs de la loi européenne proposée sur l'IA, comparable. L'application restreinte de la loi proposée au contexte du commerce et de l'exclusion des institutions fédérales et d'autres acteurs garantit que d'importantes lacunes existeront dans le cadre réglementaire canadien en matière d'intelligence artificielle.

La promesse de consultation à l'étape de l'élaboration de la réglementation ne sont pas un remède à l'absence de consultation par rapport au cadre établi dans la législation. Il n'y a eu aucune consultation, par exemple, sur le rôle que le ministre doit jouer en vertu de la loi, sur le rôle du commissaire aux données, sur la définition de « préjudice » et sur d'autres éléments clés de la loi proposée. L'absence de consultation signifie que les répercussions et les implications potentielles de ce projet – qui est difficile à comprendre étant donné qu'un si grand nombre de ses caractéristiques sont laissées à la réglementation – sont mal comprises. Ceci est inacceptable.

9.2 La LIAD met indûment l'accent sur les risques de préjudice pour les personnes à l'exclusion des préjudices collectifs.

Le projet de loi définit les systèmes d'IA à risque élevé en fonction de leurs répercussions sur les personnes, et non sur les groupes et les collectivités. Il tient compte des répercussions plus étroitement que la loi proposée de l'UE sur l'intelligence artificielle et que la propre *Directive du gouvernement fédéral sur la prise de décisions automatisée*s. Malgré l'introduction de la notion de « production biaisée », l'accent mis par la LIAD sur les préjudices individuels et quantifiables peut involontairement contribuer à perpétuer le déni de la discrimination systémique. Les objectifs de la LIAD sont nécessaires et importants, mais elle est nettement inférieure à la moyenne en raison de son individualisme, ce qui va à l'encontre des conceptions mondiales du préjudice collectif.

Les types de préjudices que la LIAD considère sont les suivants : le préjudice physique ou psychologique causé à une personne, des dommages aux biens d'une personne ou une perte économique pour une personne. Toutefois, la LIAD laisse planer une ambiguïté quant à ce qui pourrait être considéré comme un préjudice quantifiable. Par exemple, on pourrait imaginer un système d'IA qui établit le profil des personnes, qui recherche leurs susceptibilités personnelles afin de leur adresser des publicités ciblées ou qui, de manière générale, s'attaque aux faiblesses humaines perçues. Premièrement, comme il n'y a pas de définition de ce qu'est un système à fort impact dans le cadre de la LIAD, on ne sait pas si ce type de système correspond à cette définition. Deuxièmement, il n'est pas clair que les algorithmes manipulateurs et abusifs seraient considérés comme causant un « préjudice » au sens de la définition de la LIAD. En vertu de la LIAD, les dommages causés par les systèmes d'IA sont difficiles à quantifier.

Pour remédier efficacement aux « préjudices » dans le cadre de la LIAD, il faudrait aussi imposer aux personnes responsables de systèmes à fort impact l'obligation d'établir des mesures pour repérer, évaluer et atténuer les risques de préjudice ou de produits biaisés qui pourraient découler de l'utilisation du système. En outre, les personnes responsables de systèmes à fort impact devraient être tenues d'informer le ministre responsable si l'utilisation du système entraîne ou est susceptible d'entraîner un préjudice matériel (par exemple, lorsqu'un préjudice matériel s'est produit ou est sur le point de se produire).

9.3 **Le libellé de la LIAD est contradictoire et les pouvoirs d'application de la loi sont fragiles.**

Le traitement des données anonymisées entre la LPVPC et la LIAD crée un écart de gouvernance important en ce qui concerne la portée, la substance et le processus. En outre, les limites définitionnelles transférées de la LIAD à la LPVPC ne sont pas pertinentes, comme la définition de « renseignements personnels ». Les mécanismes d'application, y compris l'absence d'un droit privé d'action ou d'un mécanisme de plainte, sont également incomplets. L'absence d'un véritable organisme de réglementation indépendant en vertu de la LIAD va à l'encontre des conseils de l'OCDE sur la gouvernance en matière d'IA. Le manque de détails dans le cadre de surveillance et d'application de la LIAD est alarmant et il ne faut pas que l'objectif de rapidité du gouvernement se réalise de façon bâclée.

9.4 **La LIAD se concentre de manière inappropriée sur une gamme trop étroite de techniques algorithmiques.**

La LIAD ne réglemente que l'utilisation d'un « système d'intelligence artificielle », qu'elle définit comme « un algorithme génétique, un réseau neuronal, l'apprentissage machine ou une autre technique ». C'est beaucoup plus étroit que la définition beaucoup plus inclusive trouvée dans la loi proposée par l'UE, l'IA, qui couvre un large éventail de techniques algorithmiques, y compris celles qui sont largement utilisées depuis des décennies. La LIAD passe donc à côté de bon nombre des préjudices potentiels qu'elle est censée couvrir, comme ceux causés par l'amplification algorithmique de messages haineux, sensationnalistes ou de manipulation politique qui sèment la discorde et qui ne dépendent pas nécessairement du petit ensemble de techniques nouvelles et sophistiquées énumérées dans sa définition de l'IA.

9.5 **Reprenez l'élaboration de la LIAD, mais ne la confiez pas uniquement à ISDE**

a) Les parlementaires doivent montrer la voie

Étant donné la grande confusion quant à la nature de l'« intelligence artificielle », exacerbée par des allégations excessives et très médiatisées sur ses capacités, ses avantages potentiels et ses préjudices éventuels, la tâche initiale est d'éduquer tant les législateurs que le public en général. Les experts de l'industrie, les chercheurs, les juristes et les organisations de la société civile, en particulier celles qui représentent les parties prenantes et les communautés les plus susceptibles d'être menacées, ont un rôle important à jouer pour clarifier les questions en jeu.

La LIAD doit faire l'objet de consultations supplémentaires pour répondre aux besoins d'aujourd'hui et de demain. Pour faciliter ces consultations, un groupe de travail parlementaire composé de représentants de tous les partis pourrait être mis sur pied pour examiner les principes généraux, le cadre, la gouvernance appropriée, les mécanismes de surveillance, la définition des systèmes d'IA à incidence élevée et les zones interdites possibles de la LIAD. Dans le cadre d'un tel exercice, il serait

judicieux de commander des rapports de recherches de fond, de publier un livre blanc et de tenir une véritable consultation publique. Comme dans le cas de *la loi sur l'IA* de l'UE, certains des aspects plus techniques de la réglementation de l'IA pourraient être laissés à l'appréciation des experts et traités dans les règlements de la LIAD et/ou les normes de l'industrie.

b) Le gouvernement fédéral doit progresser

La mise en œuvre de systèmes d'IA à grande échelle peut avoir des conséquences sociétales importantes qui dépassent de loin le cadre du mandat d'ISDE. Par conséquent, d'autres ministères et organismes gouvernementaux doivent également jouer un rôle formateur dans l'élaboration de la LIAD. Une telle collaboration à l'échelle du gouvernement peut s'appuyer sur les travaux actuels menés par Justice Canada et Affaires mondiales Canada, soutenus par le Secrétariat du Conseil du Trésor et ISDE dans le cadre des négociations du Canada avec le Conseil de l'Europe (**COE**) en vue d'élaborer un traité sur l'IA qui accorde une place importante aux droits de la personne, à la démocratie et à l'État de droit. Le projet de travail consolidé de la convention-cadre fournit des éléments utiles pour le régime canadien en matière d'IA. Le régime réglementaire du Canada en matière d'IA devrait être conforme à la convention une fois qu'elle aura été ratifiée. Toutefois, les dispositions générales, les obligations et les principes du projet de convention correspondent davantage aux objectifs de prévention des dommages, d'instauration de la confiance et de promotion de l'intérêt public que tout ce qu'ISDE a rendu public jusqu'à présent. D'autres ministères ont manifestement une contribution à apporter, notamment Emploi et développement social Canada (travail), Sécurité publique (cybersécurité) et Patrimoine canadien (créateurs de contenu et artistes). Le Commissariat à la protection de la vie privée a également un rôle important à jouer, bien que négligé jusqu'à présent.

c) Convoquer une assemblée nationale de citoyens sur la gouvernance de l'IA

La consultation publique pourrait prendre la forme d'une assemblée nationale de citoyens sur la gouvernance de l'IA, qui ferait l'objet d'une large publicité. Le groupe de travail assurerait la coordination de cette assemblée, qui lui rendrait compte, lui ferait part des témoignages recueillis et lui transmettrait d'autres documents. L'OCDE recommande d'avoir recours à des assemblées de citoyens, qui permettent un engagement significatif des citoyens et une prise de décision fondée sur des données probantes pour aborder des questions complexes et difficiles. De telles assemblées ont été utilisées avec succès dans de nombreux territoires, y compris au Canada[19]. Les assemblées de citoyens canadiens sur l'expression démocratique, qui se sont récemment achevées et que se sont penchées sur l'incidence des technologies numériques sur la société canadienne[20], pourrait

[19] Voir ***Assemblée nationale citoyenne sur la réforme électorale.*** Des **assemblées de citoyens sur la réforme électorale ont été organisées** en Colombie-Britannique (2004) et en Ontario (2006) et elles ont été récemment approuvées par le Parti libéral fédéral.
[20] Voir Democratic Expression Démocratique

constituer un modèle intéressant pour une assemblée sur la gouvernance de l'IA. Un autre exemple est le panel d'utilisateurs de la Colombie-Britannique en rapport avec la British Columbia Services Card. L'expérience vécue avec ce panel suggère que l'expertise des citoyens contribue de façon notable à améliorer la compréhension des questions relatives à la protection de la vie privée et à la technologie[21].

Les aspects plus techniques de l'IA, malgré leur grande importance, peuvent très bien être traités uniquement dans les règlements et les normes, dont la rédaction exige des connaissances plus spécialisées. Toutefois, la loi elle-même devrait contenir des principes, des mécanismes de gouvernance et de contrôle appropriés, des définitions clés, comme l'IA à fort impact ou à haut risque, et peut-être même des zones interdites : tous des éléments que les assemblées de citoyens et les commissions parlementaires peuvent et doivent aborder[22]. En effet, étant donné le rythme rapide de l'évolution technologique, l'adoption d'une approche fondée sur des principes pour l'élaboration de la législation et de la réglementation, avec des mesures de transparence et de responsabilité appropriées, plutôt qu'une approche liée à des technologies précises, est nécessaire pour que les règles imposées par la loi soient largement comprises et acceptées, et durablement viables au fil du temps.

d) Choisir l'angle d'approche le plus large possible en matière d'IA et de ses risques potentiels

Pour favoriser une diffusion adéquate des enjeux de l'IA, les délibérations devraient adopter un angle d'approche très large en matière d'IA et de ses répercussions socio-économiques, en particulier en lien avec ses préjudices potentiels. En limitant la définition de l'IA à des techniques algorithmiques précises, comme le fait actuellement la LIAD, on détourne l'attention des questions fondamentales. La dernière version de la *loi sur l'IA* de l'UE, approuvée récemment par les principales commissions du Parlement européen, constitue un point de départ beaucoup plus approprié :

> [Traduction] « Un système d'intelligence artificielle (ou système d'IA) est un système automatisé, conçu pour fonctionner à différents degrés d'autonomie, qui est capable, pour atteindre des objectifs explicites ou implicites, de produire des résultats comme des prévisions, des

[21] Voir *Recommendations from BC Services Card User Panel*, en ligne : https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/Appendix-II-Recommendations-from-BC-Services-Card-User-Panel.pdf

[22] Il faut souligner que l'expertise technique, si elle est nécessaire pour élaborer des règlements et des normes, ne suffit pas à elle seule, surtout dans le cas de technologies puissantes comme l'IA, où l'intérêt public et la protection des droits fondamentaux de la personne sont en jeu. Les acteurs qui apportent une expertise complémentaire dans des domaines comme la bonne gouvernance, les droits de la personne et l'évaluation des répercussions sociales ou qui représentent les collectivités les plus susceptibles d'être touchées doivent avoir leur mot à dire au sein des structures qui définissent les règlements et les normes. Voir Mehwish Ansari et Vidushi Marda (5 mai 2023) *AI Act — leaving oversight to the techies will not protect rights*, **eu**observer

recommandations ou des décisions influant sur des environnements réels ou virtuels »[23].

La LIAD se concentre étroitement sur les préjudices individuels et quantifiables. Pour bien comprendre et résoudre les controverses qui entourent actuellement l'IA, il faut adopter une approche beaucoup plus large de la recension des risques qui doivent être réglementés. Un échantillon partiel comprend des préoccupations telles que la perte ou le déplacement des emplois, la discrimination sociale, la manipulation du comportement, les troubles de la santé mentale, la privation économique, l'exploitation de la main-d'œuvre, les cyberarmes et les armes létales autonomes (également appelées « robots tueurs »), les dépenses publiques abusives, la dégradation de l'environnement, les atteintes à la vie privée, le vol de la propriété intellectuelle, les menaces pour la sécurité publique dues à l'accélération de la cybercriminalité, le chantage automatisé, la porno-vengeance et d'autres arnaques[24], l'ingérence dans les élections, la concentration du pouvoir et l'érosion de la démocratie. Et c'est sans compter les risques « existentiels », tant vantés, mais spéculatifs, d'une prise de contrôle de l'humanité par l'IA.

Pour bon nombre d'entre eux, il est préférable de considérer que ce sont des risques de préjudices collectifs, et non pas individuels. Les préjudices collectifs sont répartis de façon inégale dans la société et peuvent avoir des effets cumulatifs très importants. En général, ils ne peuvent être imputés à des causes particulières ni être facilement quantifiables. Ils nécessitent des approches évaluatives plus systémiques, plus proches de l'évaluation des incidences sur l'environnement, avec une large participation des parties prenantes, et non pas des méthodes plus individualistes.

e) Collaborer et harmoniser à l'échelle internationale

Compte tenu de l'ampleur des systèmes d'IA les plus connus et de la portée mondiale des entreprises qui les commercialisent, la nécessité d'harmoniser la réglementation de l'IA à l'échelle internationale fait l'objet d'un large consensus. Le Canada participe déjà à deux initiatives internationales en matière de politique d'IA : l'Observatoire OCDE des politiques de l'IA (OECD.AI) et une initiative connexe, le Partenariat mondial sur l'intelligence artificielle (PMIA). Alors que des Canadiens issus de plusieurs secteurs, notamment le monde universitaire, les entreprises, la société civile/les ONG, le gouvernement et le secteur technique, sont actifs au sein de ces organisations, il semble que les parlementaires canadiens en soient absents[25]. La participation d'au moins quelques parlementaires canadiens à l'une de ces organisations ou aux deux serait précieuse, à la fois pour l'autoéducation et pour apporter une nouvelle perspective à l'élaboration de la

[23] Luca Bertuzzi (11 mai 2023) *AI Act moves ahead in EU Parliament with key committee vote*, EURACTIV.
[24] Exemples tirés de différents articles et vidéos de référence largement diffusés, tels que *The AI Dilemma*, *The Stochastic Parrot.*
[25] L'Observatoire OCDE des politiques de l'IA présente ici une liste de ses 433 membres, mais le PMAI n'a pas encore fourni une telle information.

politique internationale. La création un organisme international de réglementation de l'IA est une proposition récente à laquelle les parlementaires pourraient contribuer et sur laquelle ils pourraient vouloir se baser afin de faire correspondre les lois canadiennes en matière d'IA[26].

Les parlementaires canadiens pourraient aussi contribuer directement à une meilleure harmonisation internationale des politiques et des lois sur l'intelligence artificielle en unissant leurs efforts à ceux des législateurs d'autres pays. L'appel lancé récemment par les législateurs européens en faveur d'un sommet UE/États-Unis sur le contrôle de l'IA « très puissante » est une initiative particulièrement importante que les parlementaires canadiens pourraient vouloir soutenir[27]. Si cela se concrétise, le Canada devrait être mis à contribution.

C. Résumé et conclusion

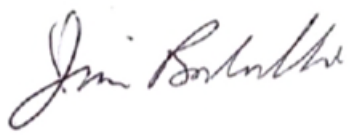
Le projet de loi C-27 ne convient pas à l'objet. Le Canada mérite beaucoup mieux pour la protection des renseignements personnels. Le projet de loi C-27 ne règle toujours pas les graves problèmes de protection de la vie privée qui sont apparus au cours des deux dernières décennies, depuis l'adoption de la LPRPDE. Il ne tient pas compte du fait que les plus importantes entreprises axées comptent sur la monétisation des renseignements personnels au moyen d'une surveillance de masse de personnes et de groupes. Ce modèle a produit une nouvelle génération de géants de la technologie d'une taille et d'une portée sans précédent, exacerbant l'asymétrie de pouvoir que ces organisations avaient déjà avec les personnes concernées. Qu'on le veuille ou non, le RGPD est généralement considéré comme la norme mondiale *de facto* pour la protection des données internationales. Le projet de loi C-27 ne correspond pas non plus aux normes mondiales contemporaines ni à la réalité actuelle de la circulation des données personnelles. Qu'on le veuille ou non, le RGPD est généralement considéré comme la norme mondiale *de facto* pour la protection internationale des données, et de nombreuses grandes entreprises doivent déjà se conformer à ses dispositions dans la mesure où elles opèrent en Europe ou traitent des données sur des citoyens européens. Le projet de loi C-27 ne correspond pas non plus aux normes mondiales contemporaines ni à la réalité actuelle de la circulation des données personnelles.

Le législateur ne devrait pas présumer que le projet de loi C-27 respectera la norme plus exigeante de l'« équivalence substantielle » lorsqu'il évaluera le caractère adéquat de la LPVPC. Nous avons l'opportunité d'adopter une loi fédérale sur la protection des renseignements personnels. Il est donc urgent que le Parlement règle ces problèmes, qu'il protège efficacement le droit à la protection de la vie privée des Canadiens et qu'il tienne les organisations responsables de leurs actes. Bon nombre des recommandations formulées dans le présent rapport s'inspirent d'exemples de pays chefs de file où une meilleure protection de la vie privée et une innovation responsable se renforcent mutuellement. D'autres recommandations sont des innovations strictement canadiennes (y compris, pour une étude plus approfondie, une recommandation qui vise à élaborer et à mettre en œuvre un nouveau cadre de gouvernance rigoureux en matière de *contrôle dès la conception*).

[26] Gary Marcus et Anka Reuel (18 avril 2023) *The world needs an international agency for artificial intelligence, say two AI experts*, The Economist.
[27] Martin Coulter et Supantha Mukherjee (17 avril, 2023) *EU lawmakers call for summit to control 'very powerful' AI*. Reuters.

Nous espérons que le gouvernement ne ratera pas cette occasion en or d'élaborer une loi avant-gardiste, adaptée aux énormes risques que posent le capitalisme de surveillance et les modèles d'affaires toxiques qu'il inspire et appuie.

Le tout respectueusement soumis,



Jim Balsillie
Fondateur, Centre pour les droits numériques

Annexe A
Autres recommandations visant à renforcer le projet de loi C-27

10.1 **Tenir les administrateurs et les dirigeants personnellement responsables.**

La LPVPC devrait tenir les administrateurs et les dirigeants personnellement responsables des SAP ou des amendes afin de promouvoir une bonne gouvernance d'entreprise et de s'assurer que les sociétés respectent leurs obligations juridiques. À défaut de le faire, les entreprises qui commettent des infractions graves à la LPRPC pourront fermer leurs portes à la suite d'une pénalité administrative et/ou d'une amende importante et rouvrir leurs portes sous une nouvelle entité (ce qui est particulièrement problématique dans le cas des entités plus petites et plus souples). La responsabilité personnelle à l'égard des amendes et des peines d'emprisonnement s'est révélée un moyen efficace de dissuasion des mauvais comportements des sociétés en vertu d'autres lois fédérales et provinciales canadiennes, y compris les infractions à la LCAP, aux lois sur la santé et la sécurité au travail et aux lois environnementales.

10.2 **Donner au commissaire à la protection de la vie privée le pouvoir de demander la restitution des profits que l'organisation tire de ses activités illégales en vertu de la LPVPC.**

La LPVPC devrait clairement prescrire un recours en restitution lié non pas à un préjudice économique traçable, mais à des violations des exigences de conception, d'exploitation et de surveillance définies publiquement.

Annexe B
Recommandations pour une étude plus approfondie

11.1 Élaborer et mettre en œuvre un nouveau cadre solide de gouvernance interne national de « contrôle dès la conception » pour réinitialiser les protections anciennes et défaillantes de la « vie privée dès la conception et par défaut » qui ont été élaborées pour la première fois au Canada dans les années 1990, et qui ont récemment pris de l'importance dans la réforme des lois sur la protection de la vie privée dans de nombreuses juridictions (y compris au Québec et dans toute l'UE), mais qui seules ne sont plus adaptées à l'usage et doivent être modernisées[28].

*Raisons du contrôle dès la conception (**CdC**)*

La gouvernance numérique est l'enjeu politique le plus important de notre époque. Nous avons subi, et continuons de subir, une transformation numérique, qui se traduit par une dépendance à l'infrastructure d'Internet et des télécommunications pour l'échange ouvert et rapide de renseignements. Cette transformation soulève des questions transversales concernant les valeurs, la distribution de la richesse, la préservation des marchés concurrentiels, la protection de la vie privée, la préservation de la santé, le maintien de l'intégrité du processus démocratique et la sécurité nationale.

La gouvernance numérique est une question de contrôle. Quiconque contrôle les données et les algorithmes qui les traitent, contrôle les personnes qui interagissent avec elles et ce qui interagit avec elles. Actuellement, nous ne contrôlons pas nos propres données. Nous « consentons » à la collecte et à l'utilisation de nos données personnelles dans le but d'utiliser un produit ou un service et nos données décollent pour le Far West. Les données recueillies peuvent être traitées et analysées de façon algorithmique de multiples façons qui ne sont généralement pas bien comprises par le sujet au moment de la collecte. On parle de la chaîne d'approvisionnement des courtiers en données et de la source de données pour le capitalisme de surveillance.

Le traitement des données d'une manière nouvelle et imprévue a d'importantes répercussions sur la sécurité, la démocratie et l'économie mondiale. Le manque actuel de contrôle personnel et démocratique sur les données et les pratiques algorithmiques dans l'économie numérique a entraîné des effets négatifs de plus en plus répandus, sur des groupes plus larges, en particulier parmi les populations vulnérables, y compris les enfants.

Nous devons mettre à jour nos lois et nos institutions inadéquates afin qu'elles soient équipées pour faire face au pouvoir de marché de ceux qui utilisent des données et des algorithmes à grande échelle.

[28] La norme ISO (ISO-31700-1) et le rapport technique (ISO TR-31700-2) de janvier 2023 concernant le respect de la vie privée dès la conception ont été examinés et il a été déterminé qu'ils ne nécessitaient pas d'ajustement aux présentes recommandations.

Il y a deux décennies, le concept de *« vie privée dès la conception et par défaut »* était une innovation bien intentionnée qui visait à améliorer la protection de la vie privée (à une époque où la plupart des organisations considéraient la protection de la vie privée comme une préoccupation secondaire ou n'y pensaient pas du tout). Bien qu'aujourd'hui ces outils aient encore une certaine portée pour soutenir un minimum d'hygiène de la protection de la vie privée par les organisations et le contrôle par les individus de leurs renseignements personnels (RP), la protection de la vie *privée dès la conception et par défaut,* en soi, est tout à fait insuffisante pour régler les asymétries structurelles et la logique économique d'exploitation qui sont en jeu dans l'économie d'aujourd'hui axée sur les données et dominée par le modèle d'affaires toxique du capitalisme de surveillance.

C'est parce que le « concepteur » est l'organisation. Par exemple, même la politique de confidentialité de Facebook indique qu'elle intègre la confidentialité dans ses produits dès le départ. Son bilan démontre le contraire. Un dénonciateur de Facebook a expliqué dans le Wall Street Journal que Facebook sait déjà, en détail, que ses plateformes causent des dommages par leur conception, souvent de façon que seule Facebook comprend parfaitement.

Nature du contrôle dès la conception (CdC)

Essentiellement, CdC est un cadre de gouvernance dans lequel les pouvoirs démocratiquement responsables (**PDR**) ou les responsables de la gérance des données (comme les services publics de données qui relèvent du gouvernement ou les fiducies de gérance des données qui ont la responsabilité de servir à la fois les sujets de données et l'intérêt public) contrôlent les ensembles de données importantes sur les renseignements personnels. CdC imposerait à ces délégués une responsabilité fiduciaire équivalant à l'éthique de « ne pas nuire » du serment d'Hippocrate.

Le CdC est explicitement aligné sur les objectifs du projet de loi C-27, qui vise à mettre en œuvre la *Charte numérique* - plus particulièrement le principe 3, Contrôle et consentement : *Les Canadiens auront le contrôle sur les données qu'ils partagent, qui utilise leurs données personnelles et à quelles fins, et ils sauront que leur vie privée est protégée.*

Le CdC est une approche fondée sur le contrôle de la gouvernance numérique, qui impose aux responsables de la gérance des données l'obligation d'agir dans l'intérêt des propriétaires des données personnelles – les Canadiens eux-mêmes. Les PDR contrôleraient également ce qui et qui interagit avec les données. Une organisation n'a pas à posséder de données pour les contrôler. Une personne ayant une obligation fiduciaire ou de nature fiduciaire envers une personne ne pourrait manifestement pas autoriser une utilisation de données qui causerait ou pourrait vraisemblablement causer un préjudice.

Le CdC pourrait stimuler l'innovation et la concurrence dans le secteur de la technologie, par exemple, les PDR pourraient établir des bassins de données ou des fiducies de données pour le bien public.

Le CdC n'est pas un modèle où les organisations continuent d'administrer elles-mêmes des ensembles de données personnelles importants. Il met fin au règne des organisations qui font « des vœux pieux » en faveur de la « vie privée dès la conception et par défaut ». Il s'attaque également au cœur du modèle d'affaires toxique que le capitalisme de surveillance inspire et soutient.

S'il était élaboré et mis en œuvre, le CdC constituerait une innovation canadienne en matière de lois et d'institutions sur la protection de la vie privée qui redonnerait au Canada la place qui lui revient en tant que pionnier mondial en matière de protection de la vie privée.

11.2 Établir une responsabilité fiduciaire qui impose des obligations de loyauté et de diligence aux organisations qui recueillent et utilisent des renseignements personnels auprès de personnes dans des circonstances où il y a un déséquilibre important des pouvoirs et de l'information ou où les personnes ne sont pas en mesure d'assurer la conformité.

Il s'agirait là d'une extension naturelle et logique des obligations fiduciaires en droit canadien. Les affaires portant sur l'obligation fiduciaire devant les tribunaux canadiens portent régulièrement sur des questions de confidentialité. Les obligations fiduciaires découlent des dépendances et des déséquilibres de pouvoir, dans des circonstances de confiance et de confidentialité. Les clients et les patients dépendent de leurs avocats et de leurs médecins - des professionnels dotés de privilèges et de pouvoirs dans les systèmes juridiques et médicaux qui font défaut aux clients et aux patients. Ils confient leurs renseignements personnels à leurs avocats et à leurs médecins, qui doivent maintenir la confidentialité des renseignements personnels, sous peine de sanctions sévères. Par conséquent, les avocats et les médecins ont en soi des obligations fiduciaires.

La situation n'est pas différente pour de nombreuses organisations, comme les plateformes de médias sociaux. Comme les clients et les patients le font avec leurs professionnels, les utilisateurs des médias sociaux confient leurs RP aux plateformes, en s'attendant raisonnablement à un certain degré de confidentialité. Les utilisateurs renoncent au contrôle sur les RP et, par conséquent, dépendent des plateformes pour utiliser leurs pouvoirs de contrôle et d'utilisation responsable. Les obligations fiduciaires restreindraient les opérations intéressées et les comportements inconsidérés de ceux qui recueillent, utilisent et communiquent des RP dans la fonction et la conception de leurs produits et services. Plus le déséquilibre entre le pouvoir et l'information d'une personne et de l'organisation est grand, plus les personnes sont vulnérables en raison de l'exposition de leurs RP, et plus le devoir auquel l'organisation de confiance doit être tenue est élevé. Les enfants sont un exemple de groupe de personnes vulnérables qui dépendent des organisations et qui leur font confiance pour respecter leurs obligations en matière de protection de la vie privée, mais qui n'ont pas le pouvoir de les faire respecter ou même de les surveiller.

Les juristes américains sont engagés dans un débat sur les « fiduciaires de l'information ». Certains estiment qu'il est nécessaire d'imposer des obligations fiduciaires. D'autres voient cette perspective comme problématique. Le droit canadien des fiducies est plus étendu que celui des États-Unis. Le débat américain pourrait donc avoir moins de résonance ici. De

plus, l'étendue accrue des principes fiduciaires canadiens les rend plus facilement applicables à la protection de la vie privée. De telles responsabilités fiduciaires pourraient être enracinées dans la LPVPC (laissant de l'espace pour croître par voie de règlement), avec une disposition concernant les obligations de confidentialité et de diligence d'une organisation lorsqu'elle est chargée de RP, selon les lignes suivantes (tirées de l'article 122 de la *Loi canadienne sur les sociétés* par actions) :

> **Responsabilité fiduciaire des organisations**
>
> 1) Toute organisation qui recueille, utilise ou divulgue les renseignements personnels d'une personne, lorsqu'il existe un déséquilibre important des pouvoirs ou de l'information entre l'organisation et la personne :
>
> a) est réputée avoir l'obligation fiduciaire d'agir avec intégrité et de bonne foi au mieux des intérêts de la personne; et
>
> b) doit exercer le soin, la diligence et la compétence dont ferait preuve, en matière de protection et d'utilisation des renseignements personnels de la personne, une organisation raisonnablement prudente dans des circonstances comparables à cette fin.
>
> 2) Lorsqu'elle agit dans l'intérêt véritable de la personne en vertu de l'alinéa 1) a), l'organisation tient compte des facteurs suivants :
>
> a) [énumérer les facteurs, chacun avec un sous-paragraphe distinct]; et
>
> b) les autres facteurs prescrits [c'est-à-dire par règlement]

Les termes « déséquilibre de pouvoir » et « déséquilibre d'information » seraient clairement définis dans la loi. Essentiellement, la définition est le déséquilibre qui découle du manque de contrôle ou d'ouverture de la personne sur l'utilisation et la conservation de ses RP une fois qu'ils sont cédés à l'organisation. Les RP relèvent essentiellement ou entièrement du pouvoir de l'organisation, indépendamment des personnes. Et afin d'éviter une échappatoire évidente, l'obligation fiduciaire « se déplacerait avec les données ». En d'autres termes, si l'organisation est vendue ou fusionnée, ou si l'ensemble des données de l'organisation est transféré, l'obligation fiduciaire visant les RP demeure en place, et le nouveau propriétaire est lié par celle-ci dans la même mesure que son prédécesseur.

11.3 Fournir au Commissariat à la protection de la vie privée les fonds nécessaires pour qu'il puisse remplir correctement son mandat.

Une approche à considérer pour fournir au Commissariat un flux de revenus correspondant à son mandat est d'exiger que toutes les organisations visées par la LPVPC paient une modeste cotisation annuelle dédiée au soutien du Commissariat. Ce modèle a également l'avantage de donner au commissaire une plus grande indépendance par rapport au gouvernement en place, comme il convient pour un haut fonctionnaire du Parlement. L'une des façons de mettre en œuvre un tel modèle de revenus est d'établir les droits sur le nombre

de personnes sur lesquelles l'organisation détient des données, ainsi que sur la sensibilité des RP traités. Cela correspondrait à la charge de travail du commissaire en matière de conformité et susciterait intuitivement l'intérêt des personnes. Des calculs préliminaires suggèrent qu'une redevance per capita facilement abordable pourrait augmenter considérablement le budget du CPVP. Un autre avantage de l'obligation d'enregistrement de toutes les organisations visées par la LPVPC est qu'elle pourrait accroître la transparence de l'écosystème du courtage de données, qui est en grande partie invisible. Plus de détails sur cette approche sont présentés ci-après.

Recommandation d'étudier plus avant « les frais d'enregistrement pour soutenir l'OPC »

Bien que les défis liés à la protection de la vie privée dans l'économie des données aient explosé au cours de la dernière décennie, la capacité du commissariat à la protection de la vie privée de s'acquitter de son mandat en vertu de la LPRPDE n'a pas augmenté proportionnellement. Le déploiement efficace des nouveaux pouvoirs de la LPVPC nécessite une augmentation importante du budget du commissaire, comme il est indiqué dans le rapport annuel 2021-2022 au Parlement. Ceci est particulièrement important parce que le CPVP devra participer aux contestations judiciaires attendues lorsqu'il imposera des SAP aux contrevenants bien nantis. À moins que le gouvernement ne soit disposé à s'engager à augmenter son financement en fonction des besoins du CPVP, des sources de revenus supplémentaires seront nécessaires.

Une indication claire que le CPVP ne dispose pas de ressources adéquates est que son budget annuel a à peine augmenté au cours de la période de 2010 à 2020, oscillant autour de 25 millions de dollars par an[29]. Il a augmenté au cours des deux dernières années, passant à un peu moins de 37 millions de dollars dans le dernier budget disponible. Avec une population canadienne de plus de 38 millions d'habitants, le gouvernement fédéral dépense en moyenne un peu moins de 1 $ par personne pour appliquer ses lois sur la protection des renseignements personnels et des données dans les secteurs public et privé. À titre de comparaison, le revenu annuel moyen par utilisateur de Facebook aux États-Unis et au Canada a augmenté de façon exponentielle au cours de cette période de 10 ans, passant de 3,20 $ US à 53,56 $ au 4e trimestre de 2020[30]. Au Canada, il en coûte en moyenne plus de 1 $ US à un annonceur pour un seul utilisateur qui clique sur une publicité Google[31]. La disparité des ressources entre ceux qui monétisent les renseignements personnels et ceux qui les protègent contre les abus ne peut guère être plus marquée.

Le registre public de protection des données du Royaume-Uni offre un exemple et un modèle de travail pour le Canada[32]. Ses frais d'enregistrement aident à faire du Commissariat à l'information l'un des organismes les mieux financés au monde.

29. Basé sur l'encaisse nette fournie par le gouvernement dans les rapports annuels du CPVP.
30. Voir le graphique de Statista : *Revenu moyen par utilisateur de Facebook au 4 e trimestre de 2020, par région* ici.
31 Voir le *coût moyen par clic de Wordstream par pays* ici.
32 Règlement de 2018 sur la protection des données (frais et informations), articles 2(2)-(3), 3 (le règlement), comme l'autorise la *Loi sur la protection des données* de 2018, article 137.

Pour voir comment des droits d'inscription de base annuels modestes fondés sur le nombre de personnes et la sensibilité de leurs données pourraient générer des revenus importants pour le CPVP, envisagez ce scénario.

Chaque organisation serait tenue de déclarer le nombre de personnes correspondant à chacune de ces trois catégories :

- n^bre^ d'adultes, pour lesquels aucune information sensible n'est traitée;
- n^bre^ d'adultes, pour lesquels des informations sensibles sont traitées;
- n^bre^ de mineurs (dont les données sont intrinsèquement considérées comme « sensibles »).

Les frais d'inscription annuels pourraient être calculés à partir d'un taux de base pour mille personnes sans données sensibles de 10 $ par mille, ou 1 cent par personne et par an, avec un supplément lorsque des renseignements sensibles sont impliqués (par exemple, le double du taux de base). Voici un exemple de frais pour une variété d'organisations hypothétiques :

Type d'organisation	**n^bre^ d'adultes (pas de renseignements sensibles)**	**n^bre^ d'adultes (avec des renseignements sensibles)**	**n^bre^ de mineurs**	**Cotisation annuelle**
Petit détaillant	2K	0	0	20 $
Détaillant de taille moyenne	200K	0	0	2 000 $
Grande banque	2M	0	100K	22 000 $
Grande compagnie de téléphone	1M	1M	0	30 000 $
Important courtier de données	1M	1M	1M	50 000 $
Grande entreprise de médias sociaux	0	10M	5M	300 000 $

Évidemment, la structure des frais devrait être fondée sur les besoins de financement du CPVP et le profil de traitement des données des personnes inscrites potentielles, c'est-à-dire le nombre d'organisations et l'échelle de leurs activités de traitement des données. Cela ferait très probablement passer le taux de base des organisations à moins de un cent par sujet de données.

Dans une opinion publiée dans le *Globe and Mail*, le professeur Andrew Clement examine le principe de financement du « pollueur-payeur » pour les organismes canadiens de réglementation de la protection des renseignements personnels[33].

11.4 Envisager la mise en place d'un mécanisme de financement du règlement des plaintes pour aider à financer les procédures judiciaires engagées par des plaignants individuels ou collectifs ou par des organismes d'intérêt public cherchant à obtenir réparation contre des organisations pour des manquements allégués à la LPVPC.

Le gouvernement fédéral, inspiré des options actuellement à l'étude en Europe et des modèles déjà en place au Canada, devrait envisager d'établir un mécanisme de financement du règlement des plaintes (qui pourrait tirer des fonds des secteurs privé ou public, ou des deux) pour fournir une aide financière aux plaignants (soit des particuliers, des groupes et des organismes d'intérêt public) qui cherchent à obtenir réparation contre des organismes pour des manquements allégués à la LPVPC. Cette évolution favorable aux droits à la protection des renseignements personnels a fait l'objet d'un rapport récent de l'Organisation européenne des consommateurs (également connue sous le nom de « BEUC ») publié en novembre 2022 et intitulé *Funding of Collective Redress - Financing options in the EU and beyond* (Financement des recours collectifs - Options de financement dans l'UE et au-delà). Le Canada pourrait s'appuyer sur les recherches et les conclusions de ce rapport pour accélérer sa réflexion sur le sujet.

En outre, et plus près de nous, le gouvernement fédéral pourrait s'inspirer de la procédure du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) pour financer la participation de l'intérêt public avec des contributions directes des parties du secteur privé soumises à la procédure. Plus précisément, depuis de nombreuses années, le CRTC a mis en place une procédure qui permet aux organismes d'intérêt public qui participent à ses procédures en matière de télécommunications de demander à bénéficier d'une prise en charge des coûts. Dans des orientations récemment mises à jour (2022), le CRTC déclare qu'il considère souvent que la participation active des organismes qui représentent les intérêts des consommateurs constitue une contribution précieuse et qu'il reconnaît que ces groupes peuvent avoir besoin d'une aide financière pour participer efficacement aux procédures. Ainsi, il peut leur accorder des frais pour leur participation aux procédures en matière de télécommunications. Les demandeurs de frais doivent atteindre le seuil de contribution pour « mieux comprendre les questions examinées », ce qui prend en compte le dépôt de preuves, le fait que la contribution était ciblée et structurée et qu'elle offrait un point de vue distinct. Ce sont les parties à une procédure en matière de télécommunications, et non le CRTC, qui paient les frais.

11.5 Protéger la confidentialité et l'anonymat du plaignant tout au long du processus de plainte, y compris lors des examens judiciaires et appels.

Il n'y a rien de plus paradoxal, mais malheureux, qu'un Canadien perde son droit à la vie privée simplement en déposant une plainte ou en invoquant ce droit devant les tribunaux. Par conséquent, la LPVPC devrait reconnaître le droit des plaignants de préserver, par défaut, leur anonymat et leur confidentialité vis-à-vis du public. Ce droit s'appliquerait non seulement dans les affaires devant

[33] Clement, Andrew, « One way we could fund our privacy watchdog », *The Globe and Mail* (éd. de l'Ontario), 3 mars 2023.

le commissaire à la protection de la vie privée (et le Tribunal de la protection des renseignements personnels et des données si le gouvernement fédéral retenait le Tribunal, contrairement à la recommandation du CDN), mais également dans toutes les procédures judiciaires et les dépôts liés à la plainte relative à la protection de la vie privée, y compris les révisions judiciaires et les appels.

Il est particulièrement important de préciser dans la LPVPC le droit à l'anonymat et à la confidentialité dans les procédures judiciaires. Le « principe de la publicité des débats judiciaires » a un statut privilégié au Canada. La Cour suprême l'a affirmé à maintes reprises. Par conséquent, les procédures judiciaires sont présumées ouvertes au public.

La Cour suprême a également reconnu que la vie privée est un intérêt public important et un droit quasi constitutionnel. La Cour a souligné l'importance primordiale de la capacité d'une personne de contrôler la façon dont ses renseignements personnels sont recueillis, utilisés et communiqués.

La Cour suprême a également statué que les tribunaux peuvent faire exception au principe de la publicité des débats judiciaires si la vie privée d'une personne est sérieusement menacée.

En incluant dans la LPVPC le droit par défaut de préserver l'anonymat et la confidentialité dans toutes les procédures, on épargnerait aux plaignants du temps, des dépenses et du stress considérables nécessaires pour obtenir une ordonnance de mise sous scellés afin de contourner le principe de la publicité des débats judiciaires. Dans le monde numérique d'aujourd'hui où les décisions sont publiées en ligne, les enjeux pour les personnes et leur vie privée sont différents et beaucoup plus complexes, ce qui permet d'étayer une discussion plus générale au sujet de la vie privée et du principe de la publicité des débats judiciaires.

En l'absence d'un tel droit par défaut, il y a un risque que les plaignants potentiels soient dissuadés de porter des questions à l'attention du commissaire à la protection de la vie privée, de crainte que leurs renseignements personnels ne soient rendus publics. Il faut donc se demander si ce risque compromet le processus de protection de la vie privée et ouvre la porte à des abus, si des renseignements personnels et confidentiels dans une affaire dont est saisi le commissaire à la protection de la vie privée deviennent automatiquement publics lorsque l'affaire est portée devant les tribunaux. De tels résultats semblent aller à l'encontre de l'objet de la Loi. Au lieu de favoriser la protection de la vie privée, il pourrait mettre en péril la vie privée des plaignants potentiels.

La LPVPC n'est pas tenue d'abandonner entièrement le principe de la publicité des débats judiciaires. L'anonymat et la confidentialité seraient protégés par défaut, mais la loi pourrait prévoir une disposition de retrait. Les plaignants pourraient renoncer à cette disposition s'ils choisissaient d'être identifiés publiquement. De plus, la LPRPC pourrait permettre à un tribunal ou au commissaire à la protection de la vie privée d'ordonner que l'anonymat et la confidentialité d'un plaignant soient retirés, s'il y avait une preuve d'un intérêt impérieux à le faire (une sorte d'ordonnance de mise sous scellés inversée).

Annexe C
Résumé des plus de 40 recommandations i) visant à corriger les problèmes et ii) pour renforcer le projet de loi C-27 et iii) pour une étude plus approfondie

i) Corriger le projet de loi C-27

1. Faire en sorte que le projet de loi C-27 réponde aux défis actuels en matière de protection des renseignements personnels et soit conforme aux normes mondiales actuelles en la matière

2. Présenter correctement les objectifs du projet de loi C-27

2.1 Reconnaître la protection de la vie privée comme un droit fondamental de la personne

2.2 Modifier le nom de la loi proposée, qui passe de « *Loi sur la protection des renseignements personnels des consommateurs* » (LPRPC) à « *Loi sur la protection des renseignements personnels au Canada* » (LPRPC) ou à « *Loi canadienne sur la protection des renseignements personnels* » (LPRPC)

2.3 Consulter les peuples autochtones pour moderniser la législation canadienne sur la protection des renseignements personnels, notamment la LPRPDE

3. Aborder la question des risques pour la démocratie liés à la protection de la vie privée

3.1 Étendre expressément la portée de la LPVPC pour couvrir les partis politiques fédéraux

4. Reconnaître les risques sérieux en matière de protection de la vie privée tant pour les groupes que pour les personnes

4.1 Étendre la protection de la vie privée pour atténuer les risques pour les groupes

4.2 Définir les « renseignements sensibles » conformément au principe général de la sensibilité énoncé à l'article 12 de la *Loi 25* du Québec et aux catégories spéciales de renseignements personnels sensibles énumérées à l'article 9 du RGPD (pour assurer le caractère adéquat), mais sur une base non exhaustive et avec l'ajout de renseignements permettant la localisation

4.3 Protéger les mineurs au moyen d'exigences de confidentialité spéciales et renforcées

4.4 Énoncer clairement que certaines zones où il est interdit d'aller représentent toujours des fins inappropriées pour la collecte, l'utilisation et/ou la communication des RP d'une personne

5. Apporter des corrections aux dispositions relatives au consentement

5.1 Renforcer le consentement valide prévu à l'article 15 de la LPVPC en rétablissant l'exigence de « compréhension » prévue à l'article 6.1 de la LPRPDE

5.2 Adopter une règle relative aux « intérêts légitimes » qui place clairement les intérêts et les droits fondamentaux de la personne au-dessus des intérêts commerciaux de l'organisation dans toute évaluation de l'incidence de l'application de la règle

5.3 Éliminer le consentement implicite comme solution de rechange au consentement exprès pour la collecte, l'utilisation ou la communication autorisées de RP

5.4 Exiger un consentement explicite sur les médias numériques pour la collecte, l'utilisation ou la communication de renseignements personnels à des fins autres que celles qui sont nécessaires pour fournir un produit ou un service

5.5 Préciser que la norme appropriée pour déterminer l'impression générale de la personne moyenne lorsqu'il s'agit de déterminer si son consentement a été obtenu « de façon trompeuse » (et est donc invalide) est celle de la personne crédule et inexpérimentée par opposition à celle de la personne raisonnable

5.6 Réviser les articles 15, 16 et 18 de la LPVPC pour répondre aux préoccupations concernant les dispositions relatives au consentement soulevées dans les recommandations 5.1 à 5.5 ci-dessus

6. Utilisez tous les outils de la « boîte à outils de protection de la vie privée et des consommateurs » pour promouvoir la responsabilité

6.1 Exiger des organisations qu'elles effectuent des évaluations des facteurs relatifs à la vie privée (ÉFVP) avant l'élaboration de produits ou de services, particulièrement lorsque des technologies et des modèles d'affaires envahissants sont appliqués, lorsque des mineurs sont impliqués, lorsque des RP sensibles sont recueillis, utilisés ou divulgués et lorsque le traitement est susceptible de poser un risque élevé pour les droits et libertés des personnes

6.2 Exiger expressément que les organisations protègent la vie privée des personnes « dès la conception et par défaut » afin de s'aligner sur l'article 9.1 de la *Loi 25* du Québec et de l'article 25 du RGPD (pour aider à assurer le « caractère adéquat »)

6.3 Promouvoir l'élaboration de modèles d'intendance des données

6.4 Renforcer les mesures de sécurité

6.5 Comme la *Loi 25* du Québec, la LPVPC devrait avoir une disposition distincte pour les flux de données transfrontaliers exigeant que les organisations au Canada qui exportent des RP vers un territoire étranger aux fins de traitement doivent d'abord

effectuer une ÉFVP pour établir que les RP recevront un niveau de protection équivalent à celui du Canada

6.6 Adopter un régime plus complet régissant les tiers fournisseurs de services et de traitement de données

6.7 Imposer clairement des obligations de transparence et de responsabilité aux courtiers en données

7. Renforcer le contrôle des personnes sur leurs RP

7.1 Fournir un droit plus complet à la « mobilité » des RP (alias « portabilité »)

7.2 Limiter les exceptions au droit d'« éliminer » des RP (c'est-à-dire le droit de « supprimer », d'« effacer » ou d'« être oublié ») et fournir le droit à l'élimination en ce qui concerne « l'indexation des RP des personnes » par les moteurs de recherche dans des circonstances précises

7.3 Renforcer l'information et l'accès

7.4 Interdire aux organisations d'utiliser les systèmes SDA/IA, sous réserve d'exceptions précises et limitées, pour recueillir, utiliser ou communiquer les RP d'une personne comme fondement de leurs décisions à leur sujet afin de s'aligner sur à l'article 22 du RGPD (pour aider à assurer le « caractère adéquat »)

7.5 Donner aux personnes le droit de contester et de s'opposer au SDA/AI qui les concerne, et pas seulement un droit à la « transparence algorithmique »

7.6 Renforcer le droit privé d'action

7.7 Ajuster le régime proposé par la LPVPC pour les renseignements non identifiables afin de préciser que les organisations doivent appliquer des processus appropriés pour anonymiser et protéger ces renseignements, et ii) pour faire en sorte que les renseignements anonymisés respectent les normes énoncées dans les règlements, pour s'aligner avec la Loi 25 du Québec

8. Donner plus de mordant au commissaire à la protection de la vie privée

8.1 Supprimer le Tribunal des renseignements personnels et de la protection des données proposé

8.2 Prévoir une application plus souple

8.3 Donner au commissaire à la protection de la vie privée le pouvoir de demander l'imposition de sanctions administratives pécuniaires d'une manière semblable aux pouvoirs conférés au commissaire de la concurrence par la *Loi sur la concurrence*

8.4 Habiliter le commissaire à la protection de la vie privée à émettre des « avis d'application » et élargir les dispositions pour lesquelles le commissaire à la protection de la vie privée peut recommander des sanctions afin d'inclure les violations des éléments suivants : 12 (1) (Fins appropriées); 55 (3) (Élimination à la demande d'un particulier : Refus motivé); 73 (Plaintes et demandes de renseignements); 75 (Interdiction de réidentification); et 97 (Vérifications)

8.5 Renforcer les dispositions relatives à la collaboration et à l'échange de renseignements interorganismes entre le commissaire à la protection de la vie privée, le commissaire de la concurrence et le CRTC

8.6 Renforcer le régime de signalement

8.7 Mettre en place un programme d'autodéclaration pour les organisations

9. La Loi sur l'intelligence artificielle et les données (LIAD) comporte des lacunes fondamentales; elle nécessite des consultations appropriées et devrait être réexaminée (sans pour autant être confiée uniquement à ISDE)

9.1 La LIAD ne convient pas et est incomplète

9.2 La LIAD met indûment l'accent sur les risques de préjudice pour les personnes à l'exclusion des préjudices collectifs

9.3 La LIAD possède un libellé contradictoire et des pouvoirs d'application fragiles

9.4 La LIAD se concentre de manière inappropriée sur une gamme trop étroite de techniques algorithmiques

9.5 Reprenez l'élaboration de la LIAD, mais ne la confiez pas uniquement à ISDE

ii) Renforcer le projet de loi C-27

10.1 Tenir les administrateurs et les dirigeants personnellement responsables

10.2 Donner au commissaire à la protection de la vie privée le pouvoir de demander la restitution des profits que l'organisation tire de ses activités illégales en vertu de la LRCDAS

iii) Pour étude plus approfondie

11.1 Élaborer et mettre en œuvre un nouveau cadre solide de gouvernance interne national de « contrôle dès la conception » pour réinitialiser les protections anciennes et défaillantes de la « vie privée dès la conception et par défaut » qui ont été élaborées pour la première fois au Canada dans les années 1990, et qui ont récemment pris de l'importance dans la réforme des lois sur la protection de la vie privée dans de nombreuses juridictions (y compris au Québec et dans toute l'UE), mais qui seules ne sont plus adaptées à l'usage et doivent être modernisées de manière innovante

11.2 Établir une responsabilité fiduciaire qui impose des obligations de loyauté et de diligence aux organisations qui recueillent et utilisent des renseignements personnels auprès de personnes dans des circonstances où il existe un déséquilibre important des pouvoirs et de l'information ou où les personnes n'ont pas la capacité d'assurer la conformité

11.3 Fournir au Commissariat à la protection de la vie privée les fonds nécessaires pour qu'il puisse remplir correctement son mandat

11.4 Envisager la mise en place d'un mécanisme de financement du règlement des plaintes pour aider à financer les procédures judiciaires engagées par des plaignants individuels ou collectifs ou par des organismes d'intérêt public cherchant à obtenir réparation contre des organisations pour des manquements allégués à la LPVPC

11.5 Protéger la confidentialité et l'anonymat du plaignant tout au long du processus de plainte, y compris lors des examens judiciaires et appels

Annexe D
Détruire le mythe selon lequel une réglementation plus stricte en matière de protection de la vie privée étouffe l'innovation

Alors qu'il est souvent largement affirmé qu'une réglementation plus stricte pénalise les innovateurs, la recherche qui a voulu mesurer la relation entre la réglementation et l'innovation ne corrobore pas ces affirmations. Contrairement aux affirmations générales d'effets « étouffants » inéluctables, les chercheurs soutiennent que si la réglementation en matière de protection des renseignements personnels peut effectivement exercer une incidence sur l'innovation, la direction de ces effets dépend de la conception de la réglementation. Par exemple, les recherches nuancées et novatrices de Mme Lev-Aretz et de M. Strandburg les amènent à conclure que :

> « les affirmations générales concernant les effets étouffants de la réglementation sur la protection de la vie privée sur l'innovation sont tout simplement fausses ». Pire encore, elles détournent l'attention des questions difficiles et importantes relatives à la conception de la réglementation. […] Une réglementation bien conçue en matière de protection des renseignements personnels a le potentiel d'améliorer la mesure dans laquelle le marché produit une gamme d'innovations socialement souhaitables »[34].

De même, les recherches de Goldfarb et de Tucker suggèrent que la réglementation sur la protection des renseignements personnels peut avoir une incidence sur l'étendue et l'orientation de l'innovation fondée sur les données, mais que les répercussions sur une telle réglementation peuvent être extrêmement hétérogènes[35]. De plus, les recherches de Martin et coll., qui ont examiné comment l'introduction du RGPD et la réglementation améliorée en matière de protection des données ont eu une incidence sur l'innovation des entreprises en démarrage en Allemagne, suggèrent que les effets d'une telle réglementation en matière de protection des renseignements personnels sont complexes : elle stimule et restreint l'innovation[36]. Les recherches d'Aridor, de Che et de Salz[37], qui ont examiné l'incidence du RGPD sur un intermédiaire de voyage en ligne, appuient la position selon laquelle la réglementation a une incidence sur les entreprises, mais n'étouffe ou ne nuit pas nécessairement aux intérêts commerciaux[38].

---

[34] Yafit Lev-Aretz et Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, Yale Journal of Law and Technology (2020) 22 : 256, en ligne : https://yjolt.org/Privacy-reglement-and-innovation-policy, p. 263.

[35] Goldfarb, Avi et Catherine E. Tucker, « Privacy and Innovation », *Innovation Policy and the Economy* (2012) 12, en ligne à l'adresse : https ://doi. org/10.1086/663156.

[36] Nicholas Martin et coll., « How Data Protection Regulation Affects Startup Innovation », *Information Systems Frontiers* (2019), 21 : p. 1307 à 1324, en ligne à l'adresse : https ://doi.org/10.1007/s10796-019-09974-2 (18 nov. 2019).

[37] Aridor, Guy, Yeon-Koo Che et Tobias Salz, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, National Bureau of Economic Research (2020), en ligne à l'adresse : https ://https://www.nber.org/papers/w26900 (révisé en mai 2021).

[38] En l'espèce, les chercheurs ont constaté que l'amélioration de la réglementation en matière de protection des renseignements personnels avait d'abord entraîné une baisse des revenus, mais que cette baisse s'était progressivement atténuée à mesure que la qualité des consommateurs qui avaient accepté de partager des renseignements après l'adoption du RGPD augmentait et que ces consommateurs étaient considérés comme ayant une valeur supérieure à celle des consommateurs d'avant le RGPD.

Le CDN est fermement convaincu que des règles rigoureuses d'équité, de responsabilité et de transparence, adaptées au contexte[39] et régissant les flux de renseignements personnels, n'étouffent pas l'innovation responsable. Elles peuvent même faire tout le contraire. Susciter la confiance bien-fondée des gens à l'égard de l'utilisation novatrice potentielle de leurs données, qu'elles soient personnellement identifiables ou anonymisées, ne peut qu'encourager l'innovation responsable.

En mai 2021, le groupe de travail sur l'innovation, la croissance et la réforme réglementaire du Royaume-Uni (le « **groupe de travail du Royaume-Uni** »)[40] a publié un rapport indépendant (le « **rapport TIGRR** »)[41] concernant des recommandations au premier ministre du Royaume-Uni sur la façon dont le Royaume-Uni pourrait redéfinir son approche en matière de réglementation afin de stimuler l'innovation, la croissance et la compétitivité. À la suite de ses consultations, le groupe de travail du Royaume-Uni a recommandé une réforme de sa loi sur la protection de la vie privée afin de donner des droits et des pouvoirs accrus aux consommateurs et aux citoyens, de responsabiliser adéquatement les entreprises qui utilisent des données et de libérer des données pour l'innovation et dans l'intérêt public. Le groupe de travail du Royaume-Uni a soutenu que la réglementation de l'économie moderne, y compris l'économie numérique, pourrait encourager la concurrence, stimuler l'innovation et promouvoir la croissance économique tout en protégeant les consommateurs et les travailleurs[42].

Le groupe de travail du Royaume-Uni a souligné que, dans le contexte de l'élaboration et de la modernisation du cadre réglementaire du Royaume-Uni, « la réglementation peut à la fois constituer un obstacle inutile à la croissance pour de nombreuses entreprises et un catalyseur pour les investissements dans de nouveaux secteurs. Une mauvaise réglementation est inefficace, coûteuse et difficile à appliquer. Une bonne réglementation, établie de la bonne façon, peut être un élément essentiel de l'infrastructure pour soutenir la croissance. En établissant des buts, des cadres et des normes clairs, proportionnels et à long terme, la réglementation du Royaume-Uni peut être un moteur important de notre compétitivité internationale[43]. »

Le groupe de travail du Royaume-Uni a également souligné qu'un manque de réglementation peut en fait étouffer l'innovation et l'investissement. Dans son rapport, le groupe de travail du Royaume-Uni a soutenu que « l'existence d'un cadre réglementaire clair pour un nouveau secteur est souvent une condition préalable essentielle à l'investissement ». Selon le groupe de travail du Royaume-Uni, le manque de clarté et le risque lié à la réglementation freinent les investissements dans certains domaines comme l'espace, la santé numérique, la mobilité en tant que service et les véhicules autonomes[44].

---

[39] Nissenbaum, Helen. *Privacy in Context, Stanford, Californie, Stanford University Press* (2009).
[40] Le groupe de travail du Royaume-Uni a consulté un large éventail d'entreprises, d'universitaires et de groupes de réflexion dans le cadre de dizaines de tables rondes et de réunions avec plus de 125 experts sur la façon dont le Royaume-Uni peut améliorer sa réglementation, aujourd'hui et à l'avenir.
[41] Taskforce on Innovation, Growth and Regulatory Reform independent report, May 2021, online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf
[42] *Ibid.*, p. 12.
[43] *Ibid.*, p. 5.
[44] *Ibid.*, p. 28.

Les recommandations du rapport TIGRR indiquent que la réglementation de l'économie numérique moderne nécessite une approche nuancée qui se concentre sur la proportionnalité des risques associés à l'innovation et aux nouvelles technologies et sur les avantages obtenus, ainsi que sur la capacité de l'organisation réglementée. Le groupe de travail du Royaume-Uni a suggéré qu'il est approprié, dans certains cas, de promouvoir l'innovation au moyen de nouvelles normes et règles adaptées spécifiquement aux PME et aux nouveaux venus[45] sur le marché, et il a reconnu qu'« il faut prendre soin d'éviter de permettre aux grandes entreprises bien établies de façonner la réglementation dans leur propre intérêt lorsque cela se fait au détriment des petits concurrents et des nouveaux venus sur le marché »[46].

Le CDN est d'accord avec la position du groupe de travail du Royaume-Uni selon laquelle la réglementation, lorsqu'elle est élaborée de façon réfléchie, peut encourager et soutenir l'innovation et permettre aux PME et aux entreprises en démarrage de concurrencer des joueurs bien établis sur le marché.

Cela dit, un document de travail de l'Université d'Oxford datant de janvier 2022 a étudié les conséquences économiques de l'introduction du RGPD sur les entreprises ciblant les consommateurs de l'Union européenne[47]. Il constate que les mesures renforcées de protection des données du RGPD et les coûts de mise en conformité qui y sont associés ont entraîné une baisse de 8 % de la rentabilité[48]. Les auteurs émettent toutefois des réserves sur leurs résultats, et ce, pour trois raisons : 1) les entreprises ont probablement encouru des coûts ponctuels pour se conformer aux nouvelles mesures, ce qui a diminué leur rentabilité, 2) à mesure que le RGPD deviendra progressivement la norme mondiale, les entreprises ciblant les consommateurs de l'Union européenne seront moins désavantagées, et 3) l'étude ne prend pas en compte les effets globaux sur le bien-être. En outre, ils affirment que « bien que l'on craigne généralement que le RGPD ait freiné l'innovation numérique en Europe, il est tout aussi plausible qu'il l'ait accélérée en incitant les entreprises à mettre au point de nouvelles technologies conformes au RGPD »[49].

Il convient également de noter que ce document de travail se concentre sur la rentabilité, et non sur l'innovation en tant que telle. Comme le notent Lev-Aretz et Strandburg, « l'innovation dans les biens et services basés sur les [renseignements personnels] n'inclut pas les améliorations qui résultent simplement de l'utilisation de « plus » de données personnelles d'une manière connue, même si elles augmentent la valeur du marché ». L'innovation qui gagne la confiance du public doit reposer sur de nouvelles pratiques d'information qui profitent non seulement aux actionnaires, mais aussi à la société en général. Des réglementations bien conçues en matière de protection des renseignements personnels peuvent contribuer à atteindre cet objectif.

---

[45] *Ibid.*, p. 6.
[46] *Idem*.
[47] Chen, Chinchih, Carl Benedikt Frey et Giorgio Presidente, Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally, Oxford Martin School, Université d'Oxford, 6 janvier 2022), en ligne à l'adresse : https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf
[48] *Ibid.*, p. 11.
[49] *Ibid.*, p. 25 et 26.

Par ailleurs, l'« effet Bruxelles" a été étudié dans le contexte du RGPD. L'« effet Bruxelles », un terme inventé par la professeure Anu Bradford, évoque l'influence de la réglementation de l'Union européenne en dehors de l'Europe, à savoir la façon dont les sociétés multinationales élèvent leurs normes réglementaires et la façon dont les normes de l'Union européenne deviennent des normes mondiales[50]. L'effet Bruxelles a joué un rôle dans l'adoption du *California Consumer Privacy Act* (CCPA)[51] et a déjà un impact sur les entreprises canadiennes dans la mesure où certaines d'entre elles traitent les données de l'Union européenne d'une manière conforme au RGPD. Le CPPA et le RGPD devraient s'aligner afin que les Canadiens ne disposent pas d'un ensemble de droits moindres[52].

[50] Bradford, Anu, The Brussels Effect: How the European Union Rules the World (2020). Columbia Law School *Faculty Books*. 232. En ligne à l'adresse : https://scholarship.law.columbia.edu/books/232
[51] Gunst, Simon, Ferdi De Ville, « The Brussels Effect: How the GDPR Conquered Silicon Valley », *European Foreign Affairs Review*, vol. 26, nº 3 (2021), p. 437 à 458, en ligne à l'adresse : https://doi.org/10.54648/eerr2021036; https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036
[52] Bennett, Colin, *One set of privacy rights for Europeans, a lesser one for Canadians? Why the Canadian consumer privacy protection act and the EU's general data protection regulation should be in alignment*, (20 mai 2021), en ligne à l'adresse : https://www.colinbennett.ca/canadian-privacy/one-set-of-privacy-rights-for-europeans-a-lesser-one-for-canadians-why-the-canadian-consumer-privacy-protection-act-and-the-eus-general-data-protection-regulation-should-be-in-alignment/

Annexe E
Critique du Centre pour les droits numériques sur les rapports de l'Association canadienne du marketing relatifs à la protection des renseignements personnels

CENTRE POUR LES DROITS NUMÉRIQUES

Le 7 mars 2023

Par courriel : asimpson@thecma.ca

Alison Simpson, présidente et chef de la direction
Association canadienne du marketing
Centre Toronto-Dominion
55 University Ave, Suite 603
Toronto (ON) M5J 2H7

Objet : La modernisation de la législation fédérale canadienne sur la protection des renseignements personnels dans le secteur privé

Chère Madame Simpson,

À la fin de ma réunion du 9 janvier avec le Comité sur la protection des renseignements personnels et des données de l'ACM, votre collègue Sara Clodman a invité le Centre pour les droits numériques (**CDN**) à examiner et à commenter les rapports [1]de février 2022 et d'octobre 2022 de l'ACM (les **Rapports de l'ACM sur la protection des renseignements personnels**) concernant la modernisation de la LPRPDE.[2] La présente lettre est la réponse du CDN à cette invitation.

Résumé

De l'avis du CDN, les assises des Rapports de l'ACM sur la protection des renseignements personnels sont fondamentalement incorrectes, car ils reposent souvent sur des publications marginales dont les auteurs sont rarement des experts ou des personnes indépendantes[3]. L'ACM s'appuie sur ces rapports pour soutenir des lois et des politiques sur la protection de la vie privée

[1] Association canadienne du marketing, *Canada's Privacy Law Priorities: Better Protections for Canadians + Innovation for Economic Growth*, octobre 2022, en ligne : https://thecma.ca/docs/default-source/default-document-library/report_privacy-law-priorities-2022.pdfctAssociation canadienne du marketing, *Privacy law pitfalls: Lessons learned from the European Union*, février 2022, en ligne : https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6 (**Rapport de l'ACM sur les écueils des lois sur la protection de la vie privée**)

[2] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 , telle que modifiée.

[3] Par exemple, comme nous l'avons vu dans la section « Perplexité à l'égard du respect de la vie privée » (voir ci-dessous à partir de la page 8), pour justifier le fait de ne pas tenir compte des résultats bien documentés et réels du sondage bisannuel auprès des consommateurs du Commissariat à la protection de la vie privée, l'ACM se contente de citer l'article d'un étudiant en droit américain et le travail de moissonnage du Web d'un robot opaque d'IA qui, selon plusieurs experts canadiens respectés en matière de protection de la vie privée, a bénéficié d'une « confiance injustifiée ».

très simplistes fondées sur des mythes de l'industrie et des erreurs de logique qui trahissent une mauvaise compréhension de l'expérience de près de cinq ans avec la loi modernisée sur la protection des renseignements personnels en Europe et une méconnaissance de la richesse des travaux d'experts contemporains sur la protection des droits relatifs à la vie privée dans l'économie fondée sur les données.

Introduction

D'après la lecture que fait le CDN des Rapports de l'ACM sur la protection des renseignements personnels, l'ACM demande :

1. une approche « faite au Canada » (c'est-à-dire une approche qui n'existe pas ailleurs dans le monde); et

2. une loi complète qui n'est ni (a) semblable au *Règlement général sur la protection des données* (**RGPD**) de l'Europe, ni b) alignée sur le régime québécois, qui traite la vie privée comme un droit de la personne et sur les aspects essentiels du projet de loi 64/la loi 25 du Québec (plus précisément, les protections améliorées inspirées du RGPD lorsque les renseignements personnels traversent les frontières).

Vous avez réitéré cet appel dans votre récente lettre d'opinion publiée dans *The Hill Times* le 15 février 2023 et intitulée *It's time to do Canada's Privacy Law in the Digital Age*.

Comme vous l'avez appris lors de notre récente réunion, et pour les raisons énoncées dans la présente lettre, je suis fortement en désaccord avec cet appel de l'ACM. Il en va de même pour bon nombre des experts en matière de protection de la vie privée que le CDN consulte, y compris le professeur Colin Bennett, comme il est indiqué dans sa récente lettre d'opinion dans le *Bulletin du CIGI* intitulée *"Privacy is Like Yoga" - and Other Myths, February 8, 2023*. Le professeur Bennett a en outre récemment fait paraître une lettre d'opinion dans *The Hill Times,* intitulée : *Privacy czar's Home Depot investigation exposes weaknesses in Ottawa's new privacy bill*, 24 février 2023. Et le professeur Andrew Clement a fait paraître une lettre d'opinion dans le *Globe and Mail* intitulée « *One way we could fund our privacy watchdog* », le 2 mars 2023.

Cela dit, il semble y avoir au moins un point important sur lequel nous pourrions être d'accord : La loi canadienne sur la protection des renseignements personnels dans le secteur privé doit être modernisée sous peu. Mais il est tout aussi important de réformer correctement la LPRPDE que de faire en sorte que la nouvelle loi soit adaptée à son objet.

En conséquence, le CDN invite l'ACM à reconsidérer sa position du point de vue des individus et des groupes canadiens, et en particulier à soutenir la position selon laquelle le respect de la vie privée doit être reconnu comme un droit fondamental. Après avoir examiné les Rapports de l'ACM sur la protection des renseignements personnels, le CDN a conclu que la position de l'ACM sur la modernisation de la LPRPDE ne tient pas compte des préjudices humains et

sociaux associés au pistage massif des internautes, en particulier ceux qui touchent les mineurs et d'autres groupes vulnérables. Comme l'a dit récemment le commissaire à la protection de la vie privée du Canada, M. Dufresne :

> « La protection de la vie privée n'est pas un droit auquel nous devrions renoncer au nom de l'innovation ou du profit, ni même au nom de l'intérêt public. Dans les cas de conflit – et ceux-ci seront rares – entre le droit à la vie privée et les intérêts privés ou publics, la protection de la vie privée l'emportera.
> …
> J'ai hâte de conseiller le Parlement sur la façon d'améliorer davantage le projet de loi C-27. » [4] (nos soulignements).

Dans la présente lettre, le CDN répond aux principales critiques formulées à l'égard de la législation modernisée sur la protection des renseignements personnels qui servent de base au raisonnement des Rapports de l'ACM sur la protection des renseignements personnels, à savoir :

1. Le respect d'une législation semblable au RGPD est (a) trop coûteux et trop contraignant et (b) étouffe l'innovation; et

2. La réglementation canadienne en matière de protection des renseignements personnels ne devrait pas être trop complexe.

Discussion

Le respect de la législation sur la protection des renseignements personnels est trop coûteux et trop contraignant

Les Rapports de l'ACM sur la protection des renseignements personnels affirment que la conformité à une législation sur la protection des renseignements personnels semblable au RGPD serait trop coûteuse et trop contraignante et ils incitent les législateurs canadiens à éviter un régime de protection des renseignements personnels qui comporte des coûts financiers élevés et un fardeau réglementaire élevé. Bon nombre des arguments de l'ACM contre l'adoption d'une loi semblable au RGPD sont liés aux coûts financiers, et plus particulièrement aux coûts pour les petites et moyennes entreprises (**PME**). L'ACM cite des rapports de tiers qui affirment que les PME sont préoccupées par les coûts de la « réglementation », terme qui peut englober un large éventail de circonstances. On ne sait pas exactement dans quelle mesure cette préoccupation est attribuable à la réglementation en général plutôt qu'à des préoccupations précises concernant le coût de la nouvelle réglementation sur la protection des renseignements personnels au Canada,

[4] CPVP Canada, Discours du Commissaire à la vie privée du Canada Philippe Dufresne, *Discussion sur la vie privée : priorités, défis et possibilités,* le 25 janvier 2023, en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2023/sp-d_20230125/

où il existe déjà des lois provinciales et fédérales sur la protection des renseignements personnels.[5]

En revanche, et sur la base des résultats d'une recherche menée par des experts indépendants, le CDN ne partage pas le point de vue selon lequel une réglementation solide en matière de protection de la vie privée entrave nécessairement l'innovation (voir ci-dessous, « Une réglementation solide en matière de respect de la vie privée et l'innovation responsable »). Le CDN est plutôt d'accord avec les récentes déclarations du nouveau commissaire fédéral à la protection de la vie privée du Canada selon lesquelles la protection de la vie privée peut favoriser l'innovation et la compétitivité, rejetant le « faux choix » entre la vie privée et l'innovation.[6]

Une version modernisée de la LPRPDE exigera naturellement de procéder à l'examen des pratiques d'une organisation en matière de renseignements personnels afin d'assurer la conformité à toute nouvelle loi adoptée, qu'il s'agisse d'une solution « canadienne » ou d'une solution semblable au RGPD. On ne peut faire abstraction de l'énorme changement culturel, technologique et sociétal qui s'est produit au Canada au cours des deux dernières décennies. Ne considérer le coût d'une version modernisée de la LPRPDE que sous l'angle financier revient à adopter une conception trop étroite et, sans tenir compte du contexte plus large, on rate la cible. De nombreuses lois qui s'appliquent directement aux industries innovatrices ont à juste titre des coûts financiers et des exigences réglementaires importants à administrer (par exemple, les lois relatives à l'innocuité des médicaments et à la protection de l'environnement). Toutefois, cela ne signifie pas que ces lois ne sont pas essentielles dans une société libre et démocratique, au sein de laquelle les données sont essentielles.

De nos jours, le quotidien de chacun est très numérisé et le quotidien des mineurs est particulièrement susceptible d'encourir les effets de la numérisation des données. Qu'il s'agisse de dossiers médicaux sensibles, de dossiers scolaires, d'inscriptions sportives, de camps d'été, d'interactions entre amis en ligne, d'enregistrements auprès du gouvernement, de commentaires sur les médias sociaux ou de messages en ligne, d'applications de jeux vidéo, de passe-temps en ligne, de cours en ligne ou de premiers comptes bancaires, la quantité de données numériques personnelles créées aujourd'hui sur les enfants et les jeunes Canadiens est sans précédent. Selon le CDN, tous les Canadiens ont droit au respect de leur vie privée et il *devrait* y avoir un coût de conformité pour s'assurer que les renseignements sensibles de mineurs et d'autres personnes et groupes vulnérables soient protégés efficacement par la loi. À cela s'ajoute l'omniprésence des atteintes à la protection des données informatiques et des acteurs malveillants qui menacent de dévoiler les données sensibles de millions de personnes. Il ne suffit pas de dire dans le projet de loi C-27 que les renseignements relatifs aux mineurs contenus sont « sensibles ».

Selon le CDN, les mineurs doivent être protégés par des exigences précises et améliorées en matière de protection de la vie privée. La *Loi sur la protection de la vie privée des*

[5] Voir le Rapport de l'ACM sur les écueils des lois sur la protection de la vie privée, à la page 3.
[6] *Supra, note* 3.

consommateurs (**LPVPC**) proposée devrait contenir des mesures visant à mettre un frein aux pratiques d'organisations en ce qui concerne la surveillance en ligne et la manipulation comportementale de mineurs. La LPVPC devrait promouvoir des protections ciblées pour les enfants et les jeunes, comme la définition de règles de consentement adaptées à l'âge et la fourniture d'un code de pratique complet pour les organisations qui collectent, utilisent ou divulguent les renseignements personnels des enfants (comme le *Children's Code* de septembre 2020 du Royaume-Uni et le *California Age-Appropriate Design Code Act* de septembre 2022).

Les autorités de protection de la vie privée ont besoin d'un financement suffisant

Bien que les commissaires à la protection de la vie privée du Canada aient publié plusieurs documents d'orientation et qu'ils aient des unités spécialisées dans les services-conseils aux entreprises, le CDN convient avec l'ACM que les organismes de réglementation de la protection de la vie privée ont besoin de fonds suffisants pour administrer et mener à bien efficacement leur mandat. Dans sa Déclaration sur le projet de loi C-27 [7] d'octobre 2022 (**la déclaration du CDN sur le projet de loi C-27**), le CDN recommande de mener une étude plus approfondie sur la façon de s'assurer que le Commissariat à la protection de la vie privée (**CPVP**) dispose d'un financement suffisant.

La déclaration du CDN sur le projet de loi C-27 recommande également de supprimer le projet de Tribunal de la protection des données et des renseignements personnels, dont la mise en œuvre et l'administration seraient coûteuses, d'autant plus qu'il existe déjà un régime en place au sein du CPVP. Aucune justification (innovation en droit de protection de la vie privée ou autre) n'a été donnée pour un tel tribunal. Son rôle et sa composition soulèvent de sérieuses préoccupations (notamment une complexité, des délais et de l'incertitude inutiles pour les personnes et les organisations dans le règlement d'une plainte. En outre, aucun régime de droit en matière de protection de la vie privée au monde n'a établi un tribunal comme le Tribunal proposé en vertu du projet de loi C-27 (y compris dans l'Union européenne, en Californie, en Utah, au Colorado, en Virginie et au Connecticut et aux termes du projet de loi américain qui s'intitule *American Data Privacy and Protection Act*). L'Australie, qui a publié un rapport le 16 février 2023 sur sa *Privacy Act*, n'a pas non plus demandé la création d'un tribunal comme celui prévu dans le projet de loi C-27, mais a plutôt proposé d'accorder des pouvoirs accrus au Commissaire à la protection de la vie privée et aux tribunaux.[8]

La création proposée du Tribunal entraînerait également des retards inutiles et compliquerait le règlement des plaintes. Vous avez peut-être pris connaissance de la récente décision du First Tier Tribunal du Royaume-Uni (le **Tribunal du Royaume-Uni**) concernant un avis d'exécution émis

[7] Centre pour les droits numériques, *Ne convient pas à l'objet – Le Canada mérite beaucoup mieux*, Déclaration du Centre pour les droits numériques sur le projet de loi C-27, 28 octobre 2022, en ligne : https://centrefordigitalrights.org/files/document/2022-11-13/257-013312.pdf
[8] Gouvernement australien, Ministère du procureur général, *Privacy Act Review Report 2022*, en ligne : https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

par l'Information Commissioner's Office (**ICO**) du Royaume-Uni.[9] Tout d'abord, l'avis faisait suite à une enquête de deux ans menée par l'ICO. Après l'enquête, il a fallu une année supplémentaire au Tribunal du Royaume-Uni pour fixer la date des audiences, puis environ 2,5 ans entre le moment de l'avis et la date de la décision du Tribunal du Royaume-Uni. Et l'affaire est toujours en cours puisque l'ICO doit décider s'il interjettera appel de la décision devant les tribunaux. Il ne fait aucun doute que « justice différée est justice refusée »; la proposition d'un Tribunal de la protection des renseignements personnels et des données dans le projet de loi C-27 devrait être abandonnée pour éviter des retards indus aux Canadiens qui exercent leurs droits à la justice.

Enfin, le CDN reconnaît que les coûts découlant du respect de la législation peuvent également être plus élevés pour les entreprises qui ne se conforment pas déjà à la LPRPDE, une loi qui prévoit actuellement de faibles sanctions financières en cas de non-conformité. Toutefois, les coûts du non-respect de la législation peuvent être beaucoup plus élevés. Il y a eu plusieurs cas en Europe et ailleurs où les GAFAM ont été lourdement mises à l'amende pour des atteintes à la vie privée.

Imposer des frais pour naviguer sur Internet?

D'après le Rapport de l'ACM sur les écueils des lois sur la protection de la vie privée, « un impact supplémentaire, qui commence à peine à se manifester dans l'univers en ligne, est que si les consommateurs fournissent moins de renseignements personnels, les entreprises envisagent d'introduire de nouveaux frais ou d'augmenter les prix actuels pour compenser la perte de revenus ».[10] Cette affirmation réitère l'argument (que de nombreux experts en protection des renseignements personnels qualifient de mythe) selon lequel la protection des renseignements personnels est un obstacle ou un compromis qui nuirait d'une certaine manière aux profits. En outre, elle s'oppose directement à la position du Commissaire fédéral à la protection de la vie privée.[11]

Il existe de nombreuses initiatives dans l'espace des technologies et de la protection des renseignements personnels, comme les technologies améliorant la confidentialité (**TAC**)[12], ainsi que des codes et des normes de conformité en matière de protection des renseignements personnels dans des domaines comme la dépersonnalisation et des méthodes novatrices pour obtenir le consentement exprès. Idéalement, les équipes du marketing et de la protection des renseignements personnels devraient collaborer pour trouver des solutions novatrices lorsqu'il est légitime de recueillir et d'utiliser des données sur les consommateurs, puisque le point de vue

[9] Voir https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/tribunal-rules-on-experian-appeal-against-ico-action/
[10] Voir le Rapport de l'ACM sur les écueils des lois sur la protection de la vie privée, à la page 18.
[11] Supra, note 3.
[12] Blogue savoir techno du CPVP : *Technologies d'amélioration de la confidentialité pour les entreprises*, (12 avril 2021), en ligne : https://www.priv.gc.ca/fr/blogue/20210412/

du consommateur concerne à la fois la protection des renseignements personnels et le marketing. Les deux n'exigent pas nécessairement de réaliser des compromis.

En outre, le CDN estime que certaines pratiques en matière de données sont inappropriées. La déclaration du CDN sur le projet de loi C-27 fait valoir que la LPVPC devrait être modifiée afin d'énoncer clairement que certaines zones où il est interdit d'aller représentent toujours des fins inappropriées pour la collecte, l'utilisation et/ou la communication des renseignements personnels d'une personne physique. Ces objectifs et interdictions inappropriés devraient inclure 1) le microprofilage psychographique et le microciblage à des fins de persuasion ou d'influence sur le comportement et 2) la capture de données biométriques sans consentement exprès (par exemple, le moissonnage d'images faciales à partir de sites Web, de plateformes et d'autres emplacements sur Internet).

Une réglementation solide en matière de respect de la vie privée et innovation responsable

Dans ses deux documents, l'ACM affirme qu'une réglementation sur la protection des renseignements personnels semblable au RGPD aura un effet paralysant sur l'innovation. À première vue, cette affirmation a un attrait intuitif superficiel. Si la réglementation sur la protection des données n'avait pas été aussi permissive, il est peu probable que le secteur nord-américain de la technologie publicitaire aurait atteint la taille de plusieurs centaines de milliards de dollars par année. Toutefois, le CDN estime qu'il est désormais clair qu'une grande partie de cette innovation a entraîné des coûts élevés pour les individus et la société en général. Espérons que l'ACM pourra le reconnaître et qu'elle ne s'intéresse qu'à la promotion de l'innovation responsable; de nouvelles formes de création de valeur socio-économique qui apportent des effets bénéfiques généraux.

Même si l'on adopte cette vision plus restreinte de l'innovation, l'affirmation de l'ACM va à l'encontre du consensus de la plupart des experts indépendants en protection de la vie privée qui ont étudié ses incidences économiques. De plus, lorsque le CDN a examiné les arguments à l'appui de la proposition selon laquelle une réglementation solide en matière de protection des renseignements personnels réduit l'innovation, il a constaté que les sources sur lesquelles s'appuyait l'ACM avaient une orientation trop étroite, qu'elles étaient limitées aux groupes sectoriels intéressés et, dans la plupart des cas, qu'elles ne répondaient pas aux normes plus rigoureuses des publications de recherche universitaires évaluées par les pairs.

Par exemple, dans le Rapport de l'ACM sur les écueils des lois
sur la protection de la vie privée, sous le titre « Entraves à la capacité des organisations d'innover et de contribuer à la croissance économique », de nombreuses notes de bas de page citent des sources liées aux coûts financiers qui découlent du respect du RGPD et à l'incidence du RGPD sur les transferts de données (voir au bas des pages 10, 11, 12 et 13). Toutefois, le CDN n'a pas pu trouver de sources dans des articles universitaires ou des recherches indépendantes pour soutenir la position selon laquelle une réglementation semblable au RGPD réduirait l'innovation au Canada. De plus, ce rapport de l'ACM cite trois sources de l'industrie allemande : deux de

Bitkom[13], qui représente des entreprises dans l'espace des médias numériques/de l'économie numérique[14] et une autre de l'association de marketing allemande, DDV.[15] Le CDN demande à l'ACM de lui signaler des rapports d'experts qui sont indépendants de l'industrie (et qui par conséquent ne sont pas tombés sous l'influence des intervenants du milieu des affaires, lesquels s'opposent depuis longtemps à la modernisation des lois en matière de protection des renseignements personnels) qui appuient l'affirmation selon laquelle une réglementation semblable au RGPD réduirait l'innovation au Canada.

La déclaration du CDN sur le projet de loi C-27 comprend une annexe D intitulée : *« Détruire le mythe selon lequel une réglementation plus stricte en matière de protection de la vie privée étouffe l'innovation ».* Le CDN a examiné plusieurs articles dans des publications savantes et dans un rapport consultatif commandé par le gouvernement qui traitent des incidences économiques des mesures relatives à la protection des données. Le CDN n'a trouvé aucune preuve dans ces articles qu'une réglementation sur la protection des renseignements personnels semblable au RGPD aurait un effet paralysant sur l'innovation au Canada. Le comportement organisationnel est influencé par plusieurs facteurs, dont un seul est la protection des données. Il convient également de souligner que des études empiriques sur les effets du RGPD sur l'innovation en Europe ont été menées et que ces études affirment qu'il a eu un effet positif. [16] L'affirmation non étayée selon laquelle une loi robuste sur la protection des renseignements personnels (comme le RGPD) a une incidence négative sur l'innovation est dangereuse, en ce sens qu'elle sous-entend faussement que la protection des renseignements personnels est un compromis et un obstacle plutôt qu'un droit fondamental de la personne, ayant une valeur inhérente, et quelque chose à dûment considérer comme tel. Par exemple, il peut être innovant de créer de nouvelles applications de jeux vidéo, utilisées par des mineurs, qui, à leur tour, annoncent d'autres applications de jeux en fonction d'une analyse de l'utilisation de ces applications. Cependant, c'est une conduite prédatrice de faire de la publicité auprès des mineurs au moyen de modèles sombres, lorsqu'on reconnaît à quel point les enfants sont vulnérables à la publicité. Une telle pratique n'est pas une innovation responsable, c'est une manipulation inappropriée.

Pour être considérée comme « responsable », l'innovation ne doit pas être évaluée uniquement en termes économiques et doit inclure des biens publics plus larges. Dans sa déclaration sur le projet de loi C-27, le CDN soutient que la LPVPC devrait expressément reconnaître la protection de la vie privée comme un droit humain fondamental qui est inextricablement lié à d'autres

[13] Datenschutz setzt Unternehmen unter Dauerdruck, Bitkom, 2021., en ligne : https://www.bitkom.org/Presse/Presseinformation/Datenschutz-setzt-Unternehmen-unter-Dauerdruck Susanne Dehmel, Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO et International Datentransfers, Bitkom, 2021. en ligne : https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf

[14] https://www.bitkom.org/EN/About-us/About-us.html

[15] https://nextcloud.ddv.de/index.php/s/Cb5JZ7fsHi2rieT

[16] Niebel, Crispin, « *The impact of the general data protection Regulation on innovation and the global politic economy* », Computer Law & Security Review, volume 40, avril 2021, en ligne (derrière le modèle payant) : https://www.sciencedirect.com/science/article/abs/pii/S026736492030128X

droits et libertés fondamentaux, y compris les droits à la vie et à la liberté (autonomie personnelle et autodétermination), la liberté de pensée et d'expression, la protection contre la discrimination et la protection contre les intrusions ou la surveillance injustifiées. Une telle reconnaissance devrait être faite à la fois dans un nouveau préambule de la LPVPC elle-même (à noter que le préambule actuel, qui sans doute ne s'applique qu'à l'ensemble du projet de loi C-27, ne contient pas une telle reconnaissance) et dans l'article 5 « Objet » de la LPVPC afin de fournir une orientation claire à ceux et celles qui interprètent la LPVPC. L'ajout d'un renvoi à la protection de la vie privée comme étant un droit fondamental de la personne dans le préambule de la LPVPC à lui seul ne suffit pas; pour éviter tout doute, une inclusion précise est nécessaire dans le corps de la LPVPC pour donner un effet juridique non équivoque à l'intention du législateur que la protection de la vie privée soit reconnue comme un droit fondamental de la personne.

En Europe, le respect de la vie privée et la protection des données sont des droits fondamentaux. Le droit au respect de la vie privée figure à la fois dans la *Déclaration universelle des droits de l'homme* des Nations unies et dans le *Pacte international relatif aux droits civils et politiques* (PIDCP). Le Haut Commissariat des Nations unies aux droits de l'homme a récemment publié un rapport qui soutient le droit au respect de la vie privée à l'heure du numérique.[17] Le CDN ne comprend pas pourquoi l'ACM s'opposerait à l'adoption du droit à la protection de la vie privée comme droit de la personne au Canada. Il l'encourage à revoir sa position. En vertu du RGPD, bien que la protection de la vie privée et des données soient des droits fondamentaux, ceux-ci peuvent tout de même être restreints d'une manière justifiable lorsque cela est nécessaire et proportionnel. Par exemple, le Contrôleur européen de la protection des données (**CEPD**) a déclaré :

> La nécessité doit être justifiée par une preuve objective et constitue la première étape avant d'évaluer la proportionnalité de la restriction...le critère de proportionnalité exige que les avantages qui résultent de la restriction au droit ne soient pas contrebalancés par les inconvénients de l'exercice du droit. Autrement dit, la restriction au droit doit être justifiée. Les protections qui accompagnent une mesure peuvent appuyer la justification d'une mesure. Une condition préalable est que la mesure soit adéquate pour atteindre l'objectif envisagé. De plus, pour évaluer le traitement des données personnelles, la proportionnalité exige que seules les données personnelles qui sont adéquates et pertinentes aux fins du traitement soient recueillies et traitées. »[18]

Le modèle réglementaire selon lequel la protection des renseignements personnels est un droit fondamental de la personne confère à chacun le droit de contrôler ses renseignements personnels d'une personne et leur traitement, surtout dans le contexte des systèmes décisionnels

[17] Nations Unies, Assemblée générale, Conseil des droits de l'homme, Rapport du Haut Commissariat des Nations unies aux droits de l'homme, « Le droit au respect de la vie privée à l'ère numérique », août 2022, en ligne : https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement
[18] CEPD, en ligne : https://edps.europa.eu/data-protection/our-work/subjects/necessite-et-proportionalite_fr

automatisés/de l'intelligence artificielle, où les risques pour les droits fondamentaux (comme le droit d'être à l'abri de la discrimination et des décisions arbitraires) sont accrus.

Enfin, le 31 mars 2022, le CPVP a publié un avis juridique d'Addario Law Group LLP selon lequel une approche fondée sur les droits de la personne en matière de protection des données est constitutionnelle.[19]

Perplexité à l'égard du respect de la vie privée

Le Rapport de l'ACM sur les écueils des lois sur la protection de la vie privée s'appuie fortement sur un document du Ministre du Parlement européen (**MPE**), Axel Voss, pour étayer les problèmes apparents découlant de la prétendue complexité du RGPD.[20] Toutefois, dans les travaux de recherche qui citent le MPE Voss, il existe aussi des données probantes qui « reconnaissent que les difficultés de mise en œuvre du cadre du RGPD ne signifient pas qu'on doive approuver l'affaiblissement des règles existantes ou adopter une approche entièrement différente ». [21]

Le Rapport de l'ACM sur les écueils des lois sur la protection de la vie privée cite en outre le document intitulé *« Hey Alexa, Do Consumers Really Want More Data Privacy* écrit par Katherine Wilcox alors qu'elle était à la faculté [22]de droit) pour défendre le point de vue que le RGPD crée de la complexité pour les consommateurs.[23] L'article affirme lui-même qu'« au lieu d'analyser quatre-vingt-dix-neuf articles et plus de 200 pages de textes réglementaires complexes, cet argument est principalement étayé par des études de cas de grandes sociétés technologiques internationales axées sur la façon dont elles recueillent et utilisent les données

[19] Addario, Frank et Samara Secter, Addario Law Group LLP, « *Opinion Prepared for the Office of the Privacy Commissioner of Canada*: Validité constitutionnelle du projet de loi C-11, *Loi sur la mise en œuvre de la Charte du numérique* » (*Commissariat à la protection de la vie privée du Canada*, 31 mars 2022), en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2022/avis-c11_addario/

[20] Voss, Axel, *Fixing the GDPR: Towards Version 2.0*,, le 25 mai 2021, en ligne : https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf

[21] Pam Dixon, Ugonma Nwankwo et Michael Pisa, *Centre for Global Development, Why Data Protection Matters for Development : The Case for Strengthening Inclusion and Regulatory Capacity*, en ligne : https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and, page 5

[22] Après avoir obtenu son diplôme de la Brooklyn Law School en 2020, Mme Wilcox a travaillé brièvement comme avocate adjointe dans un cabinet d'avocats américain avant de devenir avocate interne à Epic Games en novembre 2022 (qui a récemment fait l'objet d'une importante mesure propre à assurer l'application de la loi par la Federal Trade Commission des États-Unis : Epic Games, le fabricant du jeu vidéo Fortnite, devra payer plus d'un demi-milliard de dollars (US) en raison d'allégations par la FTC d'atteintes à la vie privée et d'imposition de frais non désirés, 19 décembre 2022). Le *Brooklyn Law Journa*l est une revue éditée par des étudiants qui accepte les manuscrits non sollicités, y compris ceux rédigés par ses étudiants. Tout cela pour dire que l'article de Mme Wilcox est peut-être « une recherche et un commentaire », mais qu'il ne s'agit ni d'un travail d'expert ni d'un travail d'érudition évalué par des pairs.

[23] Wilcox, Katherine M., *Hey Alexa, Do Consumers Really Want More Data Privacy?: An Analysis of the Negative Effects of the General Data Protection Regulation*, Brooklyn Law Review, 2019. en ligne : https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=2227&context=bl

des utilisateurs ».[24] De plus, cet article américain ne semble pas refléter l'expérience canadienne, comme l'indique le dernier *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée* du CPVP (le « **Sondage du CPVP** ») de 2020-21 du CPVP :

> « Près de neuf Canadiens sur dix se disent préoccupés dans une certaine mesure par la protection de leur vie privée.
> …
> Les Canadiens s'inquiètent de l'utilisation que feront les organisations de leurs renseignements personnels en ligne.
> …
> Les Canadiens sont plus susceptibles de se sentir mal informés sur la façon dont leurs renseignements personnels sont traités par les entreprises et le gouvernement, et bon nombre d'entre eux ont l'impression d'avoir peu de contrôle sur l'utilisation de leurs renseignements personnels ».[25]

L'ACM réfère en outre à un récent sondage mené auprès des Canadiens par un robot d'IA appelé « Polly » et affirme que les Canadiens sont deux fois plus préoccupés par la cybersécurité que par la protection des données et que parmi les Canadiens qui expriment des préoccupations au sujet de la protection des données, les préoccupations au sujet de l'utilisation des renseignements personnels par le secteur public l'emportent de loin sur les préoccupations au sujet de leur utilisation commerciale. Bien que certaines des analyses de Polly concordent avec celles du Sondage du CPVP, nous avons également fait preuve de prudence en nous demandant si une confiance injustifiée a été accordée à des robots d'IA comme « Polly ».[26] En outre, certains des principaux résultats du dernier sondage du CPVP contredisent directement les principales conclusions tirées par Polly, à savoir que dans le sondage du CPVP : (1) les Canadiens ne sont que légèrement plus préoccupés par la sécurité que par la protection de la vie privée; et (2) es préoccupations des Canadiens au sujet de l'utilisation des renseignements personnels dans le secteur public ne l'emportent pas sur les préoccupations au sujet de leur utilisation dans le secteur privé.[27]

---

[24] *Ibid*, page 260.
[25] Commissariat à la protection de la vie privée du Canada, « Sondage auprès des Canadiens à propos des questions entourant la protection de la vie privée, 2020-21 (mars 2021), en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2021/por_2020-21_ca/
[26] Dubois, Elizabeth, « *Federal election 2021 : Why we shouldn't always trust 'good' political bots* », (19 septembre 2021), en ligne : https://theconversation.com/federal-election-2021-why-we-shouldnt-always-trust-good-political-bots-168137
[27] Ce sondage bisannuel commandé par le commissaire à la protection de la vie privée du Canada et mené par Phoenix Strategic Perspectives Inc. vise à mieux comprendre la mesure dans laquelle les Canadiens sont au courant, comprennent et perçoivent les enjeux liés à la protection de la vie privée. Le sondage indique que les Canadiens ne sont que légèrement plus préoccupés par la sécurité que par la protection de la vie privée (89 % à 87 %). De plus, il estime que les préoccupations des Canadiens au sujet de l'utilisation des renseignements personnels (**RP**) dans le secteur public ne l'emportent pas sur les préoccupations au sujet de l'utilisation des renseignements personnels dans le secteur privé. Les Canadiens se sentent un peu plus informés sur la façon dont leurs RP sont gérés par le secteur

L'ACM cite également un rapport de 2022 de la *Global Data and Marketing Alliance* (GDMA) intitulé « *Global Data Privacy : What the Consumer Really Thinks* [28]et affirme que davantage de Canadiens sont des « pragmatistes des données », par opposition à des « fondamentalistes des données » ou des «personnes insensibles aux données ». Ces catégories de segmentation sont désuètes et remontent au modèle de segmentation de la vie privée du professeur Alan Westin. Des études récentes remettent en question ce modèle de segmentation. Elles affirment qu'il comporte des lacunes structurelles et qu'il est trop cité :

> La segmentation de la vie privée d'Alan Westin est bien connue et souvent utilisée, mais elle ne décrit pas avec exactitude les marchés de la vie privée ou les choix des consommateurs. La segmentation divise les répondants en « fondamentalistes », « pragmatiques » et « insensibles » à l'égard du respect de la vie privée. Il décrit le consommateur moyen comme un « pragmatiste de la protection de la vie privée » qui influence les offres du marché en soupesant les coûts et les avantages des services et en faisant des choix conformes à ses préférences en matière de protection de la vie privée. Or, les méthodes de segmentation de Westin ne permettent pas d'établir que les utilisateurs sont pragmatiques en théorie ou en pratique. [29]

Fait important, selon le même rapport de la GDMA, les consommateurs aimeraient avoir plus de contrôle sur leurs renseignements personnels, continuer de rechercher la transparence comme étape préalable de la communication de ces renseignements et s'attendre de plus en plus à ce que l'industrie protège leurs renseignements.[30]

Par ailleurs, le rapport de la GDMA constate que les Européens sont de plus en plus sensibilisés au RGPD, ce qui contribue à renforcer la confiance dans le partage des données :

> « Malgré les différences entre les marchés et les groupes d'âge, la sensibilisation du public au RGPD a nettement augmenté sur les marchés européens. De telles constatations suggèrent qu'une compréhension améliorée des protections contenues dans la réglementation a contribué à encourager et à nourrir le sentiment croissant de confort et de confiance à l'égard du partage de données... »[31]

De toute évidence, malgré les difficultés reconnues à mettre en œuvre le RGPD, son adoption a suscité un sentiment de confiance accru chez les consommateurs européens à l'égard de l'utilisation de leurs renseignements personnels par les organisations, ce qui témoigne de la

public (écart de 3 %) et ils sont beaucoup plus confiants que le gouvernement fédéral respecte leurs droits à la vie privée comparativement aux entreprises privées (un écart de 18 %).

[28] https://globaldma.com/wp-content/uploads/2022/03/GDMA-Global-Data-Privacy-2022.pdf

[29]Urban, Jennifer M. & Chris Jay Hoofnagle, « The Privacy Pragmatic as Privacy Vulnerable », (*CUPS, Carnegie Mellon University Security and Privacy Institute*, 2014), en ligne : <https://cups.cs.cmu.edu/soups/2014/workshop/privacy/s1p2.pdf>.

[30] Résumé, rapport de la GDMA.

[31] Rapport de la GDMA, p. 31-32.

validité du régime de protection des données du RGPD. Loin d'être laissés perplexes face au régime du RGPD, les Européens s'en servent comme d'une balise pour protéger leurs renseignements personnels dans l'écosystème de données mondial en évolution. De plus, les effets du RGPD se font déjà sentir au-delà de l'Europe, car de nombreuses entreprises qui exercent leurs activités au Canada sont déjà obligées de se conformer à ses modalités. Les entreprises sont déjà en mesure de respecter cette norme, pourquoi le Canada devrait-il continuer d'accuser un retard?

La disposition de déclaration d'objet de la LPRPDE est désuète

Le CDN n'est pas d'accord avec l'affirmation de l'ACM voulant que la disposition de déclaration d'objet de la LPRPDE est une « force bien reconnue », puisque cette loi ne reconnaît pas la protection de la vie privée comme un droit de la personne, malgré les conclusions différentes de nombreux instruments internationaux. Le respect de la vie privée est reconnu comme un droit de la personne au Québec, de même qu'en vertu de la Convention 108+ du Conseil de l'Europe, dans le RGPD et dans un nombre croissant de pays comme le Brésil et la Corée du Sud. De plus, le précédent commissaire à la protection de la vie privée du Canada (Daniel Therrien) et l'actuel commissaire à la protection de la vie privée du Canada (Philippe Dufresne) ont tous les deux déclaré publiquement qu'ils croient fermement que la protection de la vie privée est un droit fondamental. [32]

D'après la Commission canadienne des droits de la personne : « Les droits de la personne décrivent la façon dont nous nous attendons instinctivement à être traités.... Vous n'avez rien à faire pour mériter vos droits de la personne. Vous les obtenez en venant au monde »[33] De nombreux pays/territoires dans le monde reconnaissent que la protection de la vie privée et/ou la protection des données est un droit humain fondamental. Selon le CDN, la LPVPC continue de privilégier les intérêts des personnes morales au détriment des intérêts des personnes physiques, en continuant de normaliser le capitalisme de surveillance et en ne faisant pas de la protection de la vie privée un droit fondamental de la personne.

***

Le CDN exprime sa reconnaissance à l'ACM d'avoir invité ses membres à lui faire part de leurs commentaires sur les Rapports de l'ACM sur la protection des renseignements personnels et d'avoir encouragé le débat dans le but d'établir un cadre fédéral solide pour la protection des

[32] *Supra, note 3;* Commissariat à la protection de la vie privée du Canada, Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, mai 2021, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_ethi_c11_2105/

[33] Commission canadienne des droits de la personne, « Que sont les droits de la personne? » en ligne : https://www.chrc-ccdp.gc.ca/fr/droits-de-la-personne/que-sont-les-droits-de-la-personne, page consultée en février 2023.

Annexe F
Critique du CDN à l'égard du document complémentaire d'ISDE relatif à la LIAD

Ce que le « document complémentaire » d'ISDE nous apprend : Aucune LIAD ne serait meilleure que la présente LIAD

Introduction

Le document complémentaire (**DC**) de la LIAD, publié le 13 mars 2023 par ISDE, ne fait pas avancer la cause de la LIAD. Il est déconseillé de s'appuyer sur ce document pour prendre des décisions concernant la LIAD.

La LIAD est un avant-projet de loi bâclé et antidémocratique. Concoctée précipitamment, la LIAD omet des protections essentielles pour les Canadiens et ignore des aspects clés de la réglementation en matière d'intelligence artificielle qui sont nécessaires pour l'harmonisation des règles canadiennes avec celles de l'Union européenne.

Le DA n'est pas digne de confiance en raison de son élaboration précipitée. Il indique clairement que i) la LIAD ne protégera pas (adéquatement) les Canadiens, collectivement et individuellement, et que ii) la LIAD aura pour effet de rabaisser l'importance du Canada en tant qu'acteur de la sphère technologique mondiale. Le DC révèle que la LIAD est tellement viciée qu'il serait plus prudent de remanier son texte que de se fier à cet avant-projet, même après y avoir apporté des modifications.

En termes simples, le DC souligne les failles de la LIAD qui se répartissent en trois grandes catégories :

1. Elle expose les Canadiens à de multiples préjudices.

2. Elle est profondément antidémocratique.

3. Elle constitue un revers pour le Canada et sa place sur la scène technologique internationale.

1. Exposer les Canadiens aux préjudices

On craint généralement, avec raison, qu'à défaut d'une réglementation appropriée, les développements dans le domaine de l'IA présentent de graves risques de préjudice pour les personnes, les collectivités et la société en général. D'éminentes personnalités, des chercheurs en IA, des responsables gouvernementaux, des organisations de la société civile et le grand public ont tous exprimé leur profonde inquiétude quant au fait que, si elles ne sont pas contrôlées, les applications de l'IA menacent de nombreux aspects de la vie contemporaine.

La LIAD ne protège pas les individus et les groupes contre les effets destructeurs contre lesquels ces multiples intervenants mettent en garde. Le DC passe tout simplement sous silence les préjudices potentiels.

Même si nous ne tenons pas compte des effets néfastes de la LIAD qui ne sont pas encore visibles, cette loi expose les Canadiens à de multiples risques que le DC ne prend pas en compte. Voici une liste non exhaustive de ces risques : perte d'emploi, manipulation du comportement, troubles de la santé mentale, privation économique, exploitation de la main-d'œuvre, dégradation de la sécurité, mise en œuvre d'armes autonomes, hypertrucages (« deepfakes ») et désinformation, affectation inappropriée des ressources publiques, menaces pour la sécurité publique et érosion de la démocratie.

Ces risques ne sont pas hypothétiques. Les défenseurs, les chercheurs et les utilisateurs quotidiens de la technologie les ont documentés.

Le DC ne tente pas de traiter les préjudices d'une façon exhaustive. Il en reprend quelques-uns, en partie, lorsqu'il fait référence aux « systèmes d'intérêt », ou offre les exemples très limités de la discrimination sexuelle ou raciale, et des images, sons et vidéos obtenus par hypertrucage (« deepfake ») « qui peuvent causer des préjudices à des individus ».

Mais ces exemples de préjudices sont sélectifs. Ils se concentrent sur les individus et non sur la société. Le DC ne dit rien, par exemple, sur la perspective réaliste que les géants du numérique utilisent l'IA pour enchâsser encore plus profondément leur modèle d'affaires de capitalisme mondial de surveillance. De plus, les dommages potentiels à la sécurité publique causés par les systèmes d'IA « militarisés » dont le gouvernement est informé sont étrangement absents et ne semblent pas relever de la LIAD.

Ce qui est encore plus surprenant, c'est que le DC ne dit rien des menaces que posent les systèmes fondés sur l'intelligence artificielle pour les élections au Canada et pour la démocratie en général.

Comment le DC peut-il avoir une portée aussi limitée? Des négligences dues à une élaboration hâtive? Ou encore, était-ce pour renforcer une préférence stratégique intentionnellement rigide afin de se concentrer uniquement sur les préjudices individuels les plus manifestes et d'éviter de s'attaquer à la multitude de menaces sociétales liées à l'IA? Cette dernière interprétation est cohérente avec le langage général de la LIAD qui privilégie les individus au détriment de la société dans son ensemble.

Parmi les autres omissions dans le DC figurent les préjudices causés au développement des systèmes d'IA, non pas seulement à leur utilisation ou à leurs conséquences, mais à ceux qui nous préoccupent tous, à savoir les préjudices pour la santé mentale, les préjudices quantifiables et importants et les préjudices environnementaux.

Le DC et la LIAD doivent traiter des nombreuses formes de préjudice collectif de façon globale, et ne pas se limiter aux préjudices individuels quantifiables de façon étroite.

2. Profondément antidémocratique

Le DC met en lumière à quel point la LIAD nuit profondément aux normes démocratiques canadiennes de deux façons : premièrement, en s'écartant du processus de consultation publique approprié et, deuxièmement, en combinant les fonctions de surveillance réglementaire et de promotion de l'IA dans un seul organisme : ISDE. Un conflit d'intérêts classique.

Absence de consultation adéquate

Le texte de la LIAD est apparu pour la première fois en juin 2022 dans la partie III du projet de loi C-27. Il n'y a pas eu de préavis. Il n'y a pas eu d'audiences publiques. Le silence du DC sur ce court-circuitage du processus législatif transparent, qui est fondamental pour la démocratie au Canada, est curieux.

Le fait de légiférer sans consultation publique suscite la méfiance des Canadiennes et Canadiens, particulièrement dans un domaine aussi complexe et sensible que l'IA. Le DC ne fait rien pour régler ce problème. La technologie et les grandes entreprises de technologie suscitent déjà beaucoup de méfiance. Comment le Parlement peut-il s'attendre à ce que les Canadiens fassent confiance à la LIAD ou la respectent alors qu'il les a privés du processus normal de participation à l'élaboration de cette loi?

Les caractéristiques mêmes de l'IA qui rendent impératif un processus législatif adéquat, la nouveauté, la complexité et l'expansion effrénée dans divers aspects de la vie moderne, rendent l'abandon de la consultation publique plus dangereux. Le DC doit fournir des indications sur la façon d'obtenir une pluralité de points de vue sur les questions fondamentales que le Parlement doit résoudre pour dissiper la confusion : clarifier ce qu'est réellement l'IA, dénoncer les hyperboles au sujet des dangers et des promesses de l'IA, et contrer les messages des acteurs puissants qui se précipitent pour dominer le terrain.

Conflit d'intérêts

La LIAD s'appuie sur le même ministère tant pour la surveillance réglementaire que pour la promotion et le soutien de l'IA au Canada. Le DC s'efforce d'éviter de décrire le double rôle de l'ISDE pour ce qu'il représente réellement, un conflit d'intérêts.

Le DC explique le conflit en citant le « contexte réglementaire unique de l'IA » et en affirmant que le contrôle et la promotion de l'innovation doivent « travailler en étroite collaboration dans les premières années du cadre sous la direction du ministre ». Cette affirmation est fallacieuse, car elle cite les *Principes de bonne pratique de l'OCDE en matière de politique réglementaire* pour justifier le double rôle du ministre, alors que l'OCDE recommande explicitement le contraire, à savoir d'éviter cette combinaison.

Le fait de dévier des principes de bonne gouvernance dès le départ n'est guère une base solide pour créer un régime réglementaire fiable qui protège l'intérêt public. Il faudrait beaucoup plus qu'une affirmation du DC selon laquelle « l'IA est unique » pour justifier le conflit d'intérêts d'ISDE et gagner la confiance des Canadiens à l'égard de la LIAD, surtout après qu'il ait contourné le processus normal de consultation publique.

L'absence de détails substantiels dans le DC incite à soupçonner que le ministre protège ses prérogatives et le secteur d'activité dont il fait la promotion. Cela n'augure rien de bon pour l'avenir de la LIAD.

3. Revers international

Le DC décrit à juste titre le Canada comme « un chef de file mondial dans le domaine de l'intelligence artificielle ». Il laisse entendre à tort que la LIAD se conforme aux normes de

l'Union européenne, de l'OCDE et d'autres instances internationales en matière d'intelligence artificielle. Selon cette proposition, la LIAD retire au Canada son rôle de chef de file en matière d'IA.

Premièrement, le conflit d'intérêts d'ISDE (voir ci-dessus) contrevient aux normes de l'OCDE. Selon l'OCDE, le fait de confier à un seul organisme les fonctions de développement et de réglementation d'une industrie réduit l'efficacité de l'organisme de réglementation dans l'une ou l'autre de ses fonctions, ou dans les deux, et ne suscite pas la confiance du public.

Deuxièmement, la LIAD limite sa définition d'un « système d'intelligence artificielle » à un ensemble de techniques algorithmiques beaucoup plus restreint que la *loi sur l'IA* de l'UE. La LIAD ne s'applique qu'à l'IA « à incidence élevée ».

Toutefois, la *loi sur l'IA* de l'UE couvre explicitement une vaste gamme de techniques algorithmiques à risque faible ou élevé. Les modifications apportées à la *loi sur l'IA* de l'UE définissent explicitement les termes « système d'intelligence artificielle », « risque », « risque important », « modèle de base », « système d'IA à vocation générale » et « grands modèles de formation »[53]. Par rapport la *loi sur l'IA* de l'UE, la LIAD ignore plusieurs préjudices potentiels, tels que les messages qui sèment la discorde ou la manipulation politique et qui ne dépendent pas nécessairement du petit nombre de techniques nouvelles que la LIAD énumère dans sa définition de l'IA. Ces quelques techniques sont loin d'épuiser les nombreuses pratiques algorithmiques « à incidence élevée » de longue date qui sont facilement accessibles aux acteurs malveillants ou irresponsables.

Enfin, l'accent mis par la LIAD sur les préjudices individuels plutôt que collectifs va à l'encontre du Cadre de gestion des risques de l'IA établi par le National Institute of Standards and Technology (**NIST**) des États-Unis. À la page 1 du document du NIST, on peut lire que les technologies de l'IA « posent des risques qui peuvent avoir une incidence négative sur les personnes, les groupes, les organisations, les collectivités, la société, l'environnement et la planète ». Le DC ne tient tout simplement pas compte des préjudices plus larges, ce qui crée une divergence indésirable entre les approches américaines et canadiennes en matière d'IA.

Le DC évite la dure réalité, c'est-à-dire que les définitions de la LIAD sont clairement en contradiction avec celles de l'OCDE, de l'UE et des États-Unis. Cette non-conformité risque d'entraîner un désalignement pratique qui pourrait contrecarrer l'ambition du Canada de préserver et d'accroître l'interopérabilité de notre économie des données sur les marchés internationaux.

Conclusion

Bien que le DC soit utile pour clarifier certaines des intentions du gouvernement dans certains domaines concernant la LIAD, il est loin de fournir aux parlementaires l'orientation dont ils ont besoin avant de se prononcer sur une nouvelle loi aussi importante.

[53] Voir la *loi sur l'IA* de l'UE, texte consolidé, le 11 mai 2023, en ligne : https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf(en anglais seulement)

Les nombreuses failles du DC et son manque de contenu pertinent accentuent les préoccupations selon lesquelles le gouvernement i) n'a pas fait preuve de diligence raisonnable dans l'élaboration du projet de loi, ii) n'a pas de plan viable, et iii) est en train d'entreprendre un exercice de relations publiques. Cela nous amène à conclure que, même si l'on part d'hypothèses optimistes quant à la volonté du gouvernement d'adopter des amendements en comité, il est peu probable que cela permette de corriger les lacunes fondamentales de la LIAD au niveau du processus et du fond.

La LIAD et le DA devraient être renvoyés pour être rédigés à nouveau, mais pas ISDE seul. Une telle remise à zéro permettrait une consultation publique rigoureuse et la participation active des ministères et commissions gouvernementaux concernés qui ont été ignorés lors de l'élaboration initiale. Ces deux éléments sont essentiels à l'élaboration de bonnes lois. Et comme le DC prévoit que la LIAD n'entrera pas pleinement en vigueur avant au moins 2025, un effort de rédaction sérieux et démocratique dès à présent ne retarderait pas de façon significative l'entrée en vigueur d'une loi juste sur l'IA.

De plus, il y aurait lieu pour les législateurs de se demander s'il y a des leçons à tirer (ne serait-ce qu'à titre de mesure provisoire transitoire pour pallier les principales lacunes réglementaires) de la proposition présentée le 28 mars 2023 par le Royaume-Uni concernant la gouvernance de l'IA intitulée *A pro-innovative approach to AI regulation*[54]. Plus précisément, ce livre blanc du Royaume-Uni propose une « réglementation agile » s'articulant autour de cinq principes de développement et d'utilisation responsables de l'IA[55] aux termes desquels les autorités de réglementation existantes (comme les autorités en matière de protection des renseignements personnels et de concurrence) sont expressément dirigées et habilitées à réglementer l'IA dans leurs sphères de responsabilité.

Un nouveau départ serait plus propice à l'élaboration d'une loi propre à gagner la confiance des Canadiens et à maintenir la place du Canada sur la scène mondiale de l'intelligence artificielle, au lieu d'une loi qui exige manifestement des modifications réparatrices immédiates. Une loi souple qui s'appuie sur des fondements solides vaut mieux qu'une loi mal fondée et hâtive, surtout dans le domaine de l'intelligence artificielle qui évolue rapidement, compte tenu des promesses, des risques et des incertitudes qui l'entourent.

[54] Voir, par exemple, Teresa Scassa, *Comparing the UK's proposal for AI governance to Canada's AI bill*, du 11 avril 2023.

[55] Ces principes sont les suivants : (1) sécurité, sûreté et solidité; (2) transparence et explicabilité appropriées; (3) équité; (4) responsabilité et gouvernance; (5) possibilité de contestation et réparation.

Annexe G

La critique du CDN concernant la modification apportée par le gouvernement fédéral à la Loi électorale du Canada dans le cadre du projet de loi C-47 (la loi budgétaire de 2023) visant à mettre en œuvre un « régime national, uniforme, exclusif et complet » pour la protection de la vie privée des Canadiens par les PPF.

On retrouve, dissimulée à la fin des 270 pages du budget fédéral de 2023 publié le 28 mars 2023, une proposition selon laquelle aux termes de la Loi électorale du Canada, les partis politiques fédéraux (PPF) du Canada devraient être spécifiquement assujettis à une « approche uniforme » en matière de protection de la vie privée.

> Dans le budget de 2023, le gouvernement propose de modifier la *Loi électorale du Canada* afin d'établir une approche fédérale uniforme en ce qui a trait à la collecte, à l'utilisation et à la communication de renseignements personnels par les partis politiques fédéraux, et ce, d'une manière qui remplace les lois provinciales qui se chevauchent.

Le 20 avril 2023, et pour mettre en œuvre le budget de 2023, le gouvernement a présenté le projet de loi C-47, qui a reçu la sanction royale le 22 juin 2023 et qui comprend les modifications proposées suivantes à la *Loi électorale du Canada* (maintenant en vigueur en tant qu'article 385.2) :

> 680. La *Loi électorale du Canada* est modifiée par adjonction, après l'article 385.1, de ce qui suit :
>
> Définition de renseignements personnels
>
> 385.2 (1) Malgré la définition qu'en donne le paragraphe 2(1), au présent article, renseignements personnels s'entend de tout renseignement concernant un particulier identifiable.
>
> Collecte, utilisation, communication, conservation et retrait
>
> (2) Afin de participer aux affaires publiques en soutenant la candidature et en appuyant l'élection d'un ou de plusieurs de ses membres, tout parti enregistré ou tout parti admissible de même que toute personne ou organisation agissant en son nom, notamment ses candidats, ses associations de circonscription, ses dirigeants, ses agents, ses employés, ses bénévoles et ses représentants peuvent, conformément à la politique sur la protection des renseignements personnels du parti et sous réserve de la présente loi et de toute autre loi fédérale applicable, recueillir, utiliser, communiquer et conserver des renseignements personnels ainsi que procéder à leur retrait.
>
> Objet
>
> (3) Le présent article vise à établir un régime national, uniforme, exclusif et complet applicable aux partis enregistrés et aux partis admissibles relativement à la collecte, à l'utilisation, à la communication, à la conservation et au retrait de renseignements personnels par ceux-ci.

Les Canadiens devraient être scandalisés et ils le sont effectivement. En effet, le 28 avril 2023, le chien de garde de la démocratie Open Media a lancé une pétition[56] contre cette manœuvre politique cynique et hypocrite, qui a recueilli des milliers de signatures de Canadiens et de Canadiennes.

Il convient de souligner que, dans ses observations devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles (**LCJC**) le 3 mai 2023, le commissaire à la protection de la vie privée du Canada, Philippe Dufresne, a clairement indiqué que les PPF devraient être assujettis à des obligations concrètes en matière de protection des renseignements personnels et que la proposition contenue dans le projet de loi C-47 était tout le contraire. Plus précisément, le commissaire Dufresne a dit que :

> Les modifications proposées à la *Loi électorale du Canada* dans le projet de loi C-47 n'établissent pas d'exigences minimales en matière de protection des renseignements personnels que les partis politiques doivent respecter dans le traitement des renseignements personnels ni ne prévoient une surveillance indépendante de leurs pratiques en matière de protection des renseignements personnels. Les modifications proposées permettraient plutôt aux partis politiques et à leurs organismes associés de recueillir, d'utiliser, de conserver, de communiquer des renseignements personnels et de s'en débarrasser conformément à leurs propres politiques en matière de protection des renseignements personnels, qu'ils élaborent et révisent à leur gré.
>
> Compte tenu de l'importance de la protection des renseignements personnels et de la nature délicate des renseignements recueillis, les Canadiens ont besoin et méritent un régime de protection des renseignements personnels pour les partis politiques qui va plus loin que l'autoréglementation et qui prévoit des normes valables et une surveillance indépendante pour protéger et promouvoir le droit fondamental des électeurs à la vie privée.
>
> Les partis politiques devraient être assujettis à des règles précises en matière de protection des renseignements personnels qui sont essentiellement semblables aux exigences établies pour les secteurs public et privé dans la *Loi sur la protection des renseignements personnels* et la LPRPDE, tout en étant adaptées aux fonctions uniques que jouent les partis politiques dans le processus démocratique. En d'autres termes, les exigences en matière de protection des renseignements personnels qui sont fondées sur la législation, qui sont conformes aux principes de protection des renseignements personnels reconnus à l'échelle internationale et qui comprennent le recours à un tiers indépendant ayant le pouvoir de vérifier et d'appliquer la conformité et d'offrir des recours en cas de violation (c'est nous qui soulignons)

Dans le même ordre d'idées, dans le cadre de ses observations devant le Comité sénatorial permanent des affaires juridiques et constitutionnelles, le 3 mai, le directeur général des élections du Canada, Stéphane Perrault, a exprimé les préoccupations suivantes :

> En 2018, le projet de loi C-76 a modifié la *Loi électorale du Canada* afin d'exiger que les partis publient leur propre politique en matière de protection des renseignements personnels, qui doit comprendre des énoncés indiquant le type de renseignements recueillis et la façon dont ils sont protégés et utilisés, les circonstances dans lesquelles les renseignements peuvent être vendus, la façon dont le parti recueille et utilise les renseignements personnels créés par l'activité en ligne ainsi que le nom et les coordonnées

[56] Plus précisément, la pétition se lit comme suit : « **Nous demandons au gouvernement fédéral de retirer du projet de loi C-47 la section 39, qui modifie la *Loi électorale du Canada*, et d'ajouter les partis politiques à la définition d'organisation dans le projet de loi C-27, *Loi sur la protection de la vie privée des consommateurs*, afin qu'ils soient explicitement visés par les lois canadiennes sur la protection des renseignements personnels** ».

d'une personne à qui les préoccupations en matière de protection des renseignements personnels peuvent être adressées.

Bien que ces exigences augmentent la transparence du traitement des renseignements personnels par les partis politiques, la loi ne prévoit pas de normes minimales que les partis doivent respecter. Il n'existe pas non plus de mécanisme de surveillance pour vérifier si les partis respectent le contenu de leurs politiques, ni de sanctions en cas de non-conformité.

Dans mon rapport formulant des recommandations de 2022 à la suite des 43e et 44e élections générales, j'ai recommandé que les principes de protection des renseignements personnels énumérés à l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* s'appliquent aux partis politiques enregistrés et admissibles, sous la surveillance du Commissariat à la protection de la vie privée du Canada.

En l'absence d'une application complète de ces principes, j'ai recommandé certaines exigences minimales, à savoir :

- que les Canadiens aient le droit de refuser de recevoir des communications – ou certains types de communications – de la part de partis politiques;
- qu'ils aient la possibilité de demander l'accès aux renseignements personnels inexacts détenus par les partis politiques et de les corriger; et enfin
- que les partis politiques soient tenus d'indiquer dans leurs politiques comment les renseignements personnels des électeurs peuvent être échangés (en plus de la manière dont ils sont recueillis, utilisés et vendus).

Monsieur le Président, je crois qu'une meilleure protection des renseignements personnels des électeurs contribuera à maintenir la confiance des Canadiens envers les partis politiques du Canada et, par le fait même, envers le processus électoral. Cela dit, je tiens à être clair.

Je ne crois pas qu'une réforme aussi importante de la *Loi électorale du Canada* devrait se faire dans le contexte d'un projet de loi budgétaire, mais plutôt dans le cadre d'un projet de loi distinct. (nous soulignons)

La modification du gouvernement à la *Loi électorale du Canada* dans le projet de loi C-47 n'a rien à voir avec la « protection des renseignements personnels ». Il s'agit plutôt d'un coup de force inconstitutionnel visant à permettre aux PPF de jouir de pouvoirs non réglementés sur les renseignements personnels des Canadiens. Pourquoi les PPF résistent-ils aussi farouchement à l'obligation de respecter les mêmes règles de protection de la vie privée que le reste des Canadiens? Que nous cachent les PPF?

« *Vous devez faire ce que nous disons, pas ce que nous faisons. C'est nous qui fixons les règles. Vous devez obéir, mais nous choisissons de ne pas le faire* ». Voilà qui résume bien l'attitude des PPF à l'égard de la vie privée et des renseignements personnels des Canadiens.

Quelle hypocrisie. Les Canadiens des secteurs public et privé ont l'obligation de respecter des lois rigoureuses en matière de protection de la vie privée. Toutefois, les PPF — dont les membres élaborent lesdites lois — en seraient exemptés. Comment cela peut-il être juste ou équitable?

Le fait que les PPF ne soient pas régis par une loi sur la protection des renseignements personnels est révoltant. À l'instar de Google, de Facebook et d'innombrables petites organisations au Canada, les PPF capturent, détiennent et exploitent de grandes quantités de renseignements personnels délicats et de données de profilage à propos des Canadiens : opinions politiques, contributions aux campagnes électorales, historique des votes, appartenance religieuse, situation familiale, fourchette de revenus et bien plus encore. Des lois rigoureuses régissent la façon dont les organisations canadiennes doivent rendre compte de l'utilisation de tels renseignements. Sauf les PPF. Ils n'ont de compte à rendre à personne.

La proposition faite dans le budget, la protection de la vie privée et la Loi électorale du Canada

Personne n'a été berné par la nonchalance de la dernière phrase de la proposition non budgétaire du 28 mars 2023 du gouvernement fédéral dans le budget 2023 : « … *une approche fédérale uniforme en ce qui a trait à l'utilisation et à la communication de renseignements personnels par les partis politiques fédéraux, et ce, d'une manière qui remplace les lois provinciales qui se chevauchent* ». Ces mots dissimulent une mainmise juridictionnelle des PPF, par l'intermédiaire de leurs membres élus, pour éviter de rendre des comptes, passer outre les lois provinciales sur la protection de la vie privée et conserver leurs privilèges illimités et autoconférés sur les renseignements personnels des Canadiens.

La *Loi électorale du Canada* n'est pas une loi qui porte sur la protection des renseignements personnels. Elle concerne les *élections.* Elle ne peut pas être dénaturée par les PPF pour devenir un cadre robuste régissant la collecte, l'utilisation ou la divulgation des renseignements personnels des Canadiens. C'est la fonction des lois sur la protection de la vie privée. Demander à Élections Canada de régir la protection des renseignements personnels (un sujet à l'égard duquel cet organisme n'a ni expertise ni intérêt) équivaudrait à confier aux hôpitaux le traitement des déclarations de revenus.

Les Canadiens ont droit à de solides mesures de protection de leur vie privée. Les PPF doivent être assujettis à une réglementation exhaustive en matière de protection des renseignements personnels ainsi qu'à des mesures efficaces de surveillance et de contrôle de l'application de la loi. Le Centre pour les droits numériques a préconisé de telles mesures et les préconise dans son rapport sur le projet de loi C-27. Ces mesures sont dans l'intérêt de tous.

Advenant une grave atteinte à la protection des données détenues par les PPF (qu'ils n'ont actuellement aucune obligation de signaler à une autorité publique ou à des personnes concernées) qui ferait les manchettes dans le monde entier, les Canadiens réaliseront alors l'ampleur de la collecte des renseignements personnels et de profilage réalisée par les PPF, affranchis de tout cadre robuste de protection des renseignements personnels. La confiance des Canadiens à l'égard des PPF en sera alors fortement ébranlée. Et la cote d'estime établie par les PPF sera mise en péril.

« … qui remplace … les lois provinciales » : Une mainmise sur une compétence constitutionnelle

La modification de la *Loi électorale du Canada*, désormais en vigueur, empiète sur les pouvoirs constitutionnels établis des provinces. Ce fragment du budget ne dissimulait aucunement l'intention de prétendre « [passer outre] les lois provinciales qui se chevauchent ».

La manœuvre du gouvernement – une loi visant à exempter les PPF de l'application de la même loi sur la protection des renseignements personnels à laquelle tous les autres Canadiens doivent se conformer – est non seulement hypocrite, mais elle viole aussi la Constitution du Canada et les droits démocratiques des Canadiens en vertu de la *Charte canadienne des droits et libertés*.

L'article 92 de la *Loi constitutionnelle de 1867* accorde aux provinces une compétence exclusive en matière de protection de la vie privée au titre des domaines de compétence suivants : « la propriété et les droits civils »[57] et « les matières d'une nature purement locale ou privée »[58]. C'est grâce à ces compétences que la Colombie-Britannique, l'Alberta et le Québec ont pu adopter leurs propres lois sur la protection des renseignements personnels depuis des décennies[59].

Les modifications à la *Loi électorale du Canada*, qui se veulent exclusives, quelle que soit leur formulation, constituent une intrusion inacceptable et inconstitutionnelle dans le domaine législatif provincial. Par exemple, les protections de la vie privée dont jouissent les Québécois leur seraient refusées par et pour les PPF. Les renseignements personnels privés perdraient leur caractère privé lorsqu'ils se retrouveraient entre les mains des PPF si la loi québécoise était considérée comme une « des lois provinciales qui se chevauchent ».

La *Loi électorale du Canada* régit une chose : les élections. Les lois provinciales sur la protection de la vie privée, elles aussi, régissent une chose : la protection de la vie privée, c'est-à-dire la collecte, l'utilisation et la divulgation des renseignements personnels. Il s'agit de deux mandats distincts. L'exécution de l'un de ces mandats n'entrave pas, ne devrait pas entraver et, en vertu de la Constitution, ne peut pas entraver la capacité de l'autre à réaliser son objet. Le caractère essentiel des modifications proposées à la *Loi électorale du Canada* — leur « caractère véritable » dans le langage constitutionnel — qui couvre à la fois leur objet et leur effet[60], n'est pas la tenue d'élections fédérales. Ce serait plutôt la protection de la vie privée et des renseignements personnels des électeurs. De toute évidence, en raison de ce « caractère véritable », les modifications proposées relèvent des chefs de compétence des provinces au titre

[57] *Loi constitutionnelle de 1867*, 30 et 31, Victoria, chap. 3 (R.-U.), par. 92(13).
[58] *Idem*, par. 92(16)
[59] *Personal Information Protection Act*, SBC c 63; *Personal Information Protection Act*, SA 2003, c. P-65; *Loi sur la protection des renseignements personnels dans le secteur privé*, P-39.1 (Qué.).
[60] *Chatterjee c. Procureur général de l'Ontario*, 2009 CSC 19 au par. 17*; Renvoi relatif à la Loi sur la non-discrimination génétique*, 2020 CSC 17 au par. 28; *Renvois relatifs à la Loi sur la tarification de la pollution causée par les gaz à effet de serre,*2021 CSC 11 aux par. 51 à 56.

de l'article 92 de la *Loi constitutionnelle de 1867* mentionné ci-dessus, en l'occurrence ici la propriété et les droits civils et les matières de nature purement locale ou privée.

Même la loi fédérale actuelle sur la protection de la vie privée, la *Loi sur la protection des renseignements personnels et les documents électroniques* (**LPRPDE**), ou le texte législatif proposé pour la remplacer, la *Loi sur la protection de la vie privée des consommateurs*, ne va pas jusqu'à prétendre écarter les lois provinciales sur la vie privée. Au contraire : toutes deux reconnaissent explicitement les pouvoirs provinciaux en exemptant certaines organisations dans les cas où une province a adopté des lois essentiellement similaires en matière de protection de la vie privée.

Le droit constitutionnel canadien fait la promotion d'un fédéralisme coopératif. En usurpant la fonction des lois provinciales sur la protection de la vie privée, les modifications à la *Loi électorale du Canada* vont à l'encontre du principe du fédéralisme coopératif et de la présomption selon laquelle le Parlement a l'intention que ses lois coexistent avec les lois provinciales[61]. Nous ne nous trouvons pas devant un cas de coexistence. Il s'agit plutôt d'une intrusion inconstitutionnelle.

Les lois sur la protection de la vie privée, les « organisations » et les PPF

Les obligations créées par les lois sur la protection de la vie privée s'appliquent aux organisations. La question de savoir si les PPF sont des « organisations » aux termes de ces lois est donc cruciale. Les lois provinciales et fédérales actuelles ne traitent pas les partis politiques de la même façon.

Le gouvernement fédéral exerce une compétence limitée en matière de protection de la vie privée, en vertu de ses pouvoirs en matière de trafic et de commerce que lui octroie le paragraphe 91(2) de la *Loi constitutionnelle de 1867*. Il exerce cette compétence par l'intermédiaire de la LPRPDE.

La LPRPDE définit le terme « organisation » comme suit : « S'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales[62] ». Le Commissariat à la protection de la vie privée du Canada (**CPVP**), qui administre la LPRPDE, a déclaré qu'il ne considère pas que la LPRPDE s'applique aux PPF lorsque leurs activités ne sont pas de nature commerciale.

Toutefois, le CPVP a réclamé à maintes reprises que les PPF soient assujettis aux dispositions législatives, se fondant sur « la nécessité d'assujettir les partis politiques à une loi qui comporte

[61] *Rogers Communications Inc. c. Châteauguay (Ville)*, 2016 CSC 23 au par. 38; *Québec (procureur général) c. Canada (Procureur général)*, 2015 CSC 14 au par. 17.
[62] LPRPDE, article 2.

des obligations fondées sur des principes de protection de la vie privée reconnus à l'échelle internationale, et d'assurer qu'un tiers indépendant ait l'autorité de vérifier la conformité[63] ».

Par ailleurs, la *Loi électorale du Canada* définit le terme « PPF » comme suit : « Organisation dont l'un des objectifs essentiels consiste à participer aux affaires publiques en soutenant la candidature et en appuyant l'élection d'un ou de plusieurs de ses membres[64] ».

La *Personal Information Protection Act* de la Colombie-Britannique (**PIPA de la C.-B.**) définit le terme « organisation » comme suit : « une personne, une association sans personnalité morale, une organisation syndicale, une fiducie et un organisme sans but lucratif[65] ». La PIPA de la C.-B. a été interprétée comme s'appliquant aux partis politiques fédéraux et provinciaux[66].

La *Personal Information Protection Act* de l'Alberta (**PIPA de l'Alberta**) définit une « organisation » comme suit : « une personne morale, une association sans personnalité morale, une organisation syndicale, une société de personnes ou un particulier agissant à titre commercial ». Toutefois, elle exclut expressément les partis politiques inscrits[67].

Les dispositions législatives du Québec ont été modifiées pour assujettir les partis politiques à des parties limitées de sa *Loi sur la protection des renseignements personnels dans le secteur privé*. Les modifications apportées à la loi électorale du Québec précisent clairement que les partis politiques ne peuvent recueillir ou utiliser des renseignements personnels sans consentement. Elles énoncent en outre qu'un parti politique ne peut recueillir et utiliser que les renseignements personnels d'un électeur nécessaires à des fins électorales, de financement politique ou d'activité politique.

Les activités des PPF au Québec sont généralement assujetties à la *Charte des droits et libertés de la personne*[68] du Québec (**Charte québécoise**) et au *Code civil du Québec*[69] (**Code civil**). Plus particulièrement, l'article 5 de la *Charte québécoise* énonce que toute personne a droit au respect de sa vie privée, sous réserve des restrictions prévues par la loi. Le *Code civil* reconnaît que toute personne a droit au respect de sa vie privée (article 35), prévoit des limites à la collecte, à l'utilisation et à la communication de renseignements personnels (article 37) et garantit que toute personne a droit d'accès et de rectification de ses renseignements personnels (articles 38 à 40).

[63] https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2021/an_210513/ and https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2023/parl_20230503/
[64] *Loi électorale du Canada*, article 2https://laws-lois.justice.gc.ca/fra/lois/e-2.01/
[65] PIPA de la C.-B., article 1.
[66] *Conservative Party of Canada (Re)*, 2022 BCIPC 13.
[67] PIPA de l'Alberta., article 1.
[68] CQLR c. C -12.
[69] CQLR c. C -1991.

Cette coexistence de traitements différents des partis politiques laisse entrevoir l'intérêt d'une voie d'avenir coopérative et respectueuse de la vie privée pour les PPF au lieu des modifications actuellement en vigueur à la *Loi électorale du Canada.*

En plus d'empiéter de façon inconstitutionnelle sur la compétence législative provinciale en matière de protection de la vie privée dans la province, les modifications apportées à la *Loi électorale du Canada* portent atteinte de façon injustifiée à l'article 3 de la *Charte*, plus précisément le « droit de vote » que la Cour suprême du Canada a interprété largement comme signifiant la participation significative et éclairée de Canadiens au processus électoral.

Une approche coopérative

L'obligation de se conformer aux dispositions législatives fédérales et provinciales ne représente rien de nouveau pour les organisations canadiennes, tout particulièrement dans le domaine de la protection de la vie privée. Les organisations qui exercent leurs activités partout au Canada doivent en effet se conformer à la LPRPDE, à la PIPA de la C.-B., à la PIPA de l'Alberta et à la loi québécoise sur la protection de la vie privée dans le secteur privé, selon les circonstances.

De même, les commissaires fédéraux et provinciaux à la protection de la vie privée ont fait la preuve de leur capacité de collaborer. En effet, ils ont mené des enquêtes conjointes sur des organisations exerçant leurs activités à l'intérieur et à l'extérieur des frontières, notamment TikTok, Clearview AI, Tim Hortons, Facebook, Cadillac Fairview et AggregateIQ Data Services.

Une approche coopérative similaire doit être adoptée à l'égard des PPF. Les modifications apportées à la *Loi électorale du Canada* sont perçues comme une tentative arrogante de balayer du revers de la main les pouvoirs constitutionnels des provinces et de mettre les PPF à l'abri des lois que tous les autres Canadiens doivent respecter. En ce qui concerne la loi fédérale appropriée, il n'y a aucune raison d'intérêt public pour que les pratiques de protection de la vie privée des FPP ne soient pas assujetties au projet de loi C-27, sous la surveillance et le contrôle de l'application du CPVP.

On ne saurait permettre aux PPF, par l'entremise de leurs députés au Parlement, d'écarter les pouvoirs constitutionnels des provinces en matière de protection de la vie privée d'une manière aussi éhontée. Il serait tout aussi répréhensible pour eux de tenter de le faire que pour les provinces de tenter de prendre le contrôle de Postes Canada.

Il est peu probable qu'une exemption de l'application des lois provinciales sur la protection de la vie privée accordée au PPF puisse résister aux contestations judiciaires qui s'ensuivront inévitablement. Surtout, un tel geste minerait la confiance du public dans les PPF, à un moment où elle a grandement besoin d'être renforcée.

Annexe H
Résumé des nouveaux points dans le rapport du CDN sur le projet de loi C-27 daté du 2 octobre 2023 mettant à jour la déclaration du CDN sur le projet de loi C-27 daté du 28 octobre 2022

Ce rapport développe et met à jour comme suit la déclaration du 28 octobre 2022 du CDN sur le projet de loi C-27 :

1. **Souveraineté des données autochtones** : ajout d'une nouvelle **recommandation 2.3** (sous le titre « Présenter correctement les objectifs du projet de loi C-27 ») selon laquelle le gouvernement fédéral doit consulter les peuples autochtones et reconnaître la souveraineté autochtone sur leurs données;

2. **Partis politiques fédéraux (PPF) :** ajouter dans la **recommandation 3.1** (« Étendre expressément la loi sur la protection des renseignements personnels dans le secteur privé pour qu'elle couvre les partis politiques fédéraux canadiens ») que (a) le gouvernement australien, dans son Privacy Act Review Report 2022 du ministère du procureur général publié le 16 février 2023, recommande que les partis politiques enregistrés en Australie soient assujettis à la même loi sur la protection des renseignements personnels dans le secteur privé qui régit l'ensemble des organismes du secteur privé. et que b) les modifications récentes du gouvernement fédéral à la *Loi électorale du Canada* censées prévoir une approche fédérale uniforme à l'égard de la collecte, de l'utilisation et de la divulgation par les PPF des renseignements personnels des Canadiens par un mécanisme qui prévaudrait sur les lois provinciales chevauchantes, sont non seulement hypocrites, mais constituent une violation de la Constitution et de la *Charte* du Canada;

3. **Consentement relatif aux médias numériques** : ajouter une nouvelle recommandation 5.4 (sous la rubrique « Corriger les dispositions relatives au consentement ») selon laquelle toute collecte, utilisation ou communication en ligne de renseignements personnels d'une personne à des fins autres que celles qui sont nécessaires pour fournir un produit ou un service nécessite un consentement explicite et révocable de la part de la personne, qui est distinct de son accord relativement aux conditions d'utilisation du service, de sorte que le consentement à la protection des renseignements personnels ne constitue pas une condition du service. Le présent ajout vise à refléter l'évolution de la norme en matière de collecte de données en ligne énoncée dans le cadre des décisions récentes du Comité européen de la protection des données (le 5 décembre 2022) et de l'Irish Data Commission (le 31 décembre 2022) dans les affaires *Meta Ireland* contre Facebook et Instagram, et par le Commissariat à la protection de la vie privée du Canada dans son rapport de conclusions de l'affaire intitulée *Home Depot* du 26 janvier 2023;

4. **Réécrire des dispositions sur le consentement et les intérêts légitimes de la LPVPC :** notamment dans la nouvelle **recommandation 5.5**, une proposition de réécriture des articles 15 et 18(3) de la LPVPC pour répondre aux préoccupations du CDN dans les recommandations 5.1 à 5.4;

5. **Renseignements non identifiables** : ajouter, à la **recommandation 7.7** (à la rubrique « Ajuster le régime proposé par la LPVPC pour les renseignements non identifiables »), la mention

de l'exposé du 7 décembre 2022 sur le projet de loi C-27 du Canadian Anonymization Network (**CANON**);

6. **Protection des renseignements personnels et contrôle dès la conception** : ajouter à la **recommandation 11.1** (à la rubrique « Pour une étude plus approfondie » et en ce qui concerne le concept de « contrôle dès la conception » et ses avantages par rapport à la « protection des renseignements personnels dès la conception ») la mention de la norme ISO de janvier 2023 sur la « protection des renseignements personnels dès la conception » (ISO 31700-1) et du rapport technique (ISO/RR 31700-2);

7. **Mécanisme de financement du règlement des plaintes :** ajouter comme nouvelle **recommandation 11.4** (à la rubrique « Pour une étude plus approfondie ») que le gouvernement fédéral, inspiré des options actuellement à l'étude en Europe et des modèles déjà en place au Canada, envisage d'établir un mécanisme de financement du règlement des plaintes (qui pourrait tirer des fonds des secteurs privé ou public, ou des deux) pour aider à financer les procédures judiciaires engagées par des plaignants individuels ou collectifs ou par des organismes d'intérêt public cherchant à obtenir réparation contre des organismes pour des manquements allégués à la LPVPC;

8. **Une réglementation stricte en matière de protection des renseignements personnels encourage la confiance et favorise l'innovation responsable** : ajouter à l'annexe D (« Détruire le mythe selon lequel une réglementation plus stricte en matière de protection des renseignements personnels étouffe l'innovation ») des études supplémentaires qui examinent l'impact économique du RGPD et l'« effet Bruxelles », à savoir comment la réglementation européenne peut rehausser et a rehaussé les normes mondiales;

9. **Ajouts à la bibliographie** : ajout de plusieurs publications à l'annexe I (la « bibliographie annotée ») notamment des articles d'opinion publiés par les professeurs Bennett et Clement et de nouveaux articles dont deux sont consacrés à la LIAD par le professeur Scassa;

10. **Critique de la position de l'Association canadienne du marketing (ACM) :** ajout, à titre de nouvelle **annexe E**, de la critique du CDN concernant les rapports de février et d'octobre 2022 sur la protection des renseignements personnels de l'ACM[70]. Cette critique a été préparée à la demande de l'ACM à la suite de la réunion de Jim Balsillie qui s'est tenue le 9 janvier 2023 avec le Comité sur la protection des renseignements personnels et des données de l'ACM;

[70] En plus des graves lacunes des Rapports de confidentialité de l'ACM décrites dans la lettre du CDN du 7 mars 2023 à l'ACM, après un examen minutieux des déclarations faites dans le rapport de confidentialité de février 2022 de l'ACM et des sources de ces déclarations citées dans les notes de bas de page, le CDN est d'avis que ce rapport de l'ACM en particulier (alléguant divers écueils du Règlement général sur la protection des données « RGPD ») est désuet, hors contexte et déconnecté de la réalité. Le Rapport s'appuie sur des informations dépassées et omet des faits nouveaux. Il fait fi de recherches cruciales et dresse un portrait trompeur favorisant le secteur corporatif et négligeant les consommateurs. Il n'a pas fait l'objet de recherches appropriées et indépendantes et ne devrait pas servir de fondement à la politique publique.

11. **Critique du Document complémentaire d'ISDE sur la LIAD et consultation concernant un code de pratique volontaire du secteur pour l'IA générative :** ajout à l'annexe F de la critique du CDN sur le « document complémentaire » d'ISDE sur la LIAD, publié le 13 mars 2023, neuf mois après le dépôt de la LIAD à la Chambre des communes le 16 juin 2022. Voir aussi la critique du professeur Clement concernant la consultation d'ISDE en août et septembre au sujet d'un code volontaire pour les systèmes d'IA génératifs; et

12. **Critique à l'égard des modifications apportées par le gouvernement fédéral à la *Loi électorale du Canada* afin de prévoir une « approche uniforme » des lois sur la protection de la vie privée pour les PPF :** ajout, à titre de nouvelle annexe G, de la critique du CDN, fondée sur la Constitution et la *Charte*, des modifications apportées par le gouvernement fédéral à la *Loi électorale du Canada*, annoncées le 28 mars 2023 et qui ont reçu la sanction royale le 22 juin 2023.

Annexe I
Bibliographie annotée

La présente bibliographie annotée fournit des liens vers certaines des plus récentes recherches et analyses ainsi que des renseignements supplémentaires sur bon nombre des sujets abordés dans le présent rapport. Elle vise à aider les décideurs, les intervenants, les universitaires, les professionnels et les autres parties intéressées à obtenir de la documentation supplémentaire sur des sujets liés à la modernisation de la protection des renseignements personnels.

1. Addario, Frank et Samara Secter, Addario Law Group S.E.N.C.R.L., s.r.l., « Opinion Prepared for the Office of the Privacy g of Canada: The Constitutional Validity of Bill C-11, the Digital Charter Implementation Act » (*Commissariat à la protection de la vie privée du Canada*, 31 mars 2022), en ligne : https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/op-c11_addario/

   La commissaire à la protection de la vie privée du Canada a retenu les services du cabinet Addario Law Group S.E.N.C.R.L., s.r.l. pour qu'il fournisse un avis juridique sur la constitutionnalité du projet de loi C-11, *Loi sur la mise en œuvre de la Charte numérique du Canada*. L'avis juridique concluait que, compte tenu de l'évolution de la jurisprudence sur le partage des compétences au cours des cinq dernières années et de la prévalence de l'économie numérique, un tribunal jugerait le projet de loi C-11 comme étant constitutionnel et un exercice valide du pouvoir fédéral en matière de commerce. **L'avis portait également sur les amendements proposés par le commissaire à la protection de la vie privée au projet de loi C-11, à savoir si l'ajout d'un préambule (qui incluait explicitement la reconnaissance de la vie privée comme un droit fondamental de la personne) et d'autres amendements modifiaient le caractère véritable du projet de loi au détriment de son objectif économique. L'avis a révélé qu'aucun des amendements proposés par le commissaire à la protection de la vie privée n'a modifié le caractère véritable du projet de loi et que, en fait, certains des amendements renforceront la validité constitutionnelle du projet de loi en clarifiant le rôle central de l'économie nationale dans le projet de loi et sa promotion par le biais d'une protection rigoureuse de la vie privée.**

2. Anderljung, Markus et Joslyn Barnhart, Jade Leung, Anton Korinek, Cullen O'Keefe, Jess Whittlestone, Shahar Avin, Miles Brundage, Justin Bullock, Duncan Cass-Beggs, Ben Chang, Tantum Collins, Tim Fist, Gillian Hadfield, Alan Hayes, Lewis Ho, Sara Hooker, Eric Horvitz, Noam Kolt, Jonas Schuett, Yonadav Shavit, Divya Siddarth, Robert Trager, Kevin Wolf, « Frontier AI Regulation : Managing Emerging Risks to Public Safety », (Université Cornell, juillet 2023), en ligne à l'adresse : https://arxiv.org/abs/2307.03718. Le document examine l'équilibre entre les risques pour la sécurité publique et l'innovation dans le développement et l'avancement de l'IA. Il porte sur **les modèles d'« IA d'avant-garde », c'est-à-dire des modèles susceptibles de présenter des caractéristiques dangereuses suffisantes pour constituer un risque grave pour la sécurité publique**. Trois facteurs permettent de penser que le

développement de l'IA d'avant-garde doit faire l'objet d'une réglementation ciblée : (1) les modèles peuvent présenter des caractéristiques dangereuses inattendues et difficiles à détecter; (2) les modèles déployés à grande échelle peuvent être difficiles à contrôler de façon fiable et à empêcher qu'ils soient utilisés pour causer des préjudices; et (3) les modèles peuvent proliférer rapidement, ce qui permettrait de contourner les mesures de protection. **Il est peu probable que l'autoréglementation offre une protection suffisante contre les risques liés aux modèles d'intelligence artificielle d'avant-garde, et l'intervention gouvernementale sera nécessaire. Les options d'intervention comprennent des mécanismes pour créer et mettre à jour les normes de sécurité, des mécanismes pour donner de la visibilité aux organismes de réglementation et des mécanismes pour assurer le respect des normes de sécurité**. Certaines normes de sécurité ou garde-fous comprennent la réalisation d'évaluations approfondies des risques fondées sur des évaluations des capacités dangereuses et de la capacité de contrôle, l'embauche d'experts externes pour effectuer un examen indépendant des modèles, le respect de protocoles normalisés sur la façon dont les modèles d'IA d'avant-garde peuvent être déployés en fonction de leur évaluation des risques, ainsi que la surveillance et la réponse aux nouvelles informations sur les capacités des modèles.

3. Ansari, Mehwish et Vidushi Marda, « AI Act — leaving oversight to the techies will not protect rights », (EUObserver, le 5 mai 2023), en ligne https://euobserver.com/opinion/156992

Les auteurs affirment que les deux principaux comités européens désignés dans la *loi sur l'IA* de l'UE pour élaborer des normes, des cadres techniques, des exigences et des spécifications pour les technologies d'IA à haut risque ne sont peut-être pas les mieux placés pour assurer une réelle protection des droits fondamentaux des personnes. Ils font remarquer que ces comités, le Comité européen de normalisation (CEN) et le Comité européen de normalisation électrotechnique (CENELEC), sont presque exclusivement composés d'ingénieurs ou de technologues et que les experts en droits de la personne et les organisations de la société civile n'y sont que peu ou pas du tout représentés, ce qui suscite certaines inquiétudes si l'on pense qu'ils auront de facto le pouvoir de déterminer comment la l*oi sur l'IA* sera mise en œuvre, sans pour autant disposer des moyens nécessaires pour garantir le respect des droits fondamentaux des personnes. Selon les auteurs, on ne s'intéresse pas suffisamment à la façon dont les applications « à risque élevé » des systèmes d'IA seront mises en œuvre dans la pratique, et il est impossible de séparer complètement le choix de la conception des répercussions réelles sur les droits individuels. Ils affirment que **l'externalisation de ces enjeux à des instances techniques n'est pas la solution pour réglementer l'IA d'une manière qui respecte les droits de la personne et ils suggèrent qu'une meilleure façon d'aller de l'avant serait d'élaborer des cadres d'évaluation des répercussions sur les droits fondamentaux**

auxquels seraient soumis tous les systèmes d'IA à risque élevé avant de pouvoir être mis sur le marché.

4. Balkin, Jack M., « The Fiduciary Model of Privacy », (Harvard Law Review, novembre 2020), en ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700087

   Cet article résume et reformule la théorie des fiduciaires de l'information et le modèle fiduciaire de protection de la vie privée. Il soutient qu'en **raison de la vulnérabilité et de la dépendance créées par le capitalisme de l'information, la loi devrait considérer les entreprises numériques qui recueillent et utilisent les données des utilisateurs finaux comme des fiduciaires de l'information**. Les devoirs fiduciaires « accompagnent les données » : les entreprises numériques doivent s'assurer que toute personne qui partage ou utilise les données est également digne de confiance et est légalement tenue aux mêmes exigences légales de confidentialité, de soin et de loyauté qu'elles. Les articles précisent qu'une fois mis en œuvre, **le modèle fiduciaire […] incitera les entreprises numériques à agir dans l'intérêt de leurs utilisateurs finaux**, intérêt qu'elles prétendent souvent respecter, mais qu'elles ne respectent pas. L'article se termine par une proposition visant à imposer des obligations fiduciaires aux entreprises.

5. Balsillie, Jim, « Privacy is central to human well-being, democracy, and a vibrant economy. So why won't the Trudeau government take it seriously? » The Globe and Mail, 22 octobre 2022, online : https://www.theglobeandmail.com/opinion/article-digital-privacy-technology-canada/ *[Note : Derrière le modèle payant]*

   L'auteur met en lumière les principaux défauts du projet de loi C-27 et critique ses nombreux échecs tant pour les Canadiens que pour les entreprises canadiennes, notamment le fait que, en accordant la priorité aux intérêts commerciaux du gouvernement fédéral, le projet de loi 1) normalise et étend le capitalisme de surveillance, 2) ne fait pas de la vie privée un droit humain fondamental, 3) continue de s'appuyer sur le modèle largement discrédité de la primauté du consentement, 4) crée des exceptions trop larges au consentement pour les entreprises (y compris l'exception mal conçue des « intérêts légitimes ») qui ne protègent pas la vie privée des Canadiens et ne stimulent pas l'innovation, 5) ne fait pratiquement rien pour protéger les mineurs et ignorent les lois progressistes récemment adoptées au Royaume-Uni et en Californie qui accordent une attention particulière à la protection des droits à la vie privée des enfants, et 6) ne fournit pas, dans le projet de *Loi sur l'intelligence artificielle et les données* (LIAD), même un soupçon de cadre pour une réglementation et une surveillance responsables de l'intelligence artificielle et des systèmes de décision automatisés.

6. Bannerman, Sara, Julia Kalinina, Elizabeth Dubois et Nicole Goodman, « Privacy and Canadian Political Parties : The Effects of the Data-Driven Campaign on Elector Engagement. », (*Revue canadienne de science politique* 1-24, octobre 2022), en ligne : https://doi.org/10.1017/S000842392200066X,

   Les auteurs rapportent les résultats d'un sondage examinant l'attitude des Canadiens à l'égard de la collecte de renseignements personnels par les partis politiques et son impact

potentiel sur l'engagement des électeurs. **Entre autres conclusions, les auteurs estiment que l'application de la loi sur la protection des renseignements personnels aux partis politiques est justifiée. Les résultats du sondage corroborent les opinions exprimées dans des sondages menés par le Centre pour les droits numériques et le Commissariat à la protection de la vie privée du Canada, qui ont révélé que plus de 85 % des Canadiens croient que les partis politiques devraient être assujettis à la loi sur la protection de la vie privée.**

7. Bednar, Vass, « Debating the Right Balance (s) for Privacy Law in Canada » (Public Policy Forum, January 2022), en ligne : https://ppforum.ca/publications/debating-the-right-balances-for-privacy-law-in-canada/

   Ce rapport est un résumé des tables rondes et des discussions qui ont eu lieu entre des universitaires, des avocats, des représentants du secteur privé et des membres de la société civile en vertu des règles de Chatham House. Organisées par le Forum des politiques publiques, les discussions ont porté sur des questions clés concernant la modernisation de la protection de la vie privée et la façon dont le Canada se compare aux autres régimes dans le monde. Les débats des tables rondes montrent que certains participants sont optimistes quant à la possibilité de coexister une approche axée sur les droits de la personne en matière de protection de la privée, avec une innovation du secteur privé axée sur les données. **De plus, il y avait du scepticisme quant à l'utilité d'un nouveau Tribunal de la protection de la vie privée qui pourrait être distinct de celui du commissaire à la protection de la vie privée. Le rapport note également que l'exemption des partis politiques des exigences imposées au secteur privé représente un désalignement.** Le traitement devrait être uniforme entre les organismes sans but lucratif et de bienfaisance et les partis politiques. Dans l'ensemble, les intervenants croient qu'un cadre cohérent de protection de la vie privée qui protège mieux les Canadiens et favorise l'innovation responsable est réalisable grâce à l'harmonisation des approches mises en place par les provinces canadiennes et à ce que l'on apprend des pairs internationaux qui ont ouvert la voie.

8. Bennett, Colin, « Canada Introduces Three New Privacy Bills to Modernise Privacy Law », Privacy Laws and Business, August 2022), https://www.privacylaws.com/reports-gateway/reports/ *[Note : Derrière le modèle payant.]*

   L'article porte sur la présentation de projets de loi sur la protection de la vie privée récemment déposés au Canada, soit le projet de loi C-27 et son prédécesseur, l'ancien projet de loi C-11. L'article explique comment le projet de loi C-11 a fait l'objet de critiques de la part de toutes les allégeances politiques et comment le projet de loi C-27 a fait l'objet d'importantes modifications. Toutefois, **une grande partie de l'ancien projet de loi C-11 a été conservée dans le projet de loi C-27**, ce qui a probablement déçu les défenseurs de la protection de la vie privée. L'article explique que le projet de loi C-27 ne mentionne pas expressément que la protection de la vie privée est un droit fondamental de la personne, que le cadre de protection de la vie privée fondé sur le consentement pour le traitement des données personnelles demeure et souligne les changements apportés aux

définitions des renseignements anonymisés et anonymisés. L'article décrit également la nouvelle *Loi sur l'intelligence artificielle et les données,* affirmant qu'elle a l'air d'être une sorte de « coquille vide » où il reste beaucoup à réglementer.

9. Bennett, Colin J., « Privacy czar's Home Depot investigation exposes weaknesses in Ottawa's new privacy bill », *The Hill Times,* 23 février 2023, en ligne à l'adresse : https://www.hilltimes.com/story/2023/02/23/privacy-czars-home-depot-investigation-exposes-weaknesses-in-ottawas-new-privacy-bill/379346/.

   L'auteur examine le rapport de conclusions du Commissariat à la protection de la vie privée du Canada (CPVP) dans l'affaire *Home Depot* afin de montrer les limites des dispositions du projet de loi C-27 relatives au consentement implicite. Il soutient que les dispositions relatives au consentement implicite du projet de loi C-27 devraient être supprimées, car elles créent de la confusion tant pour les consommateurs que pour les entreprises. Dans cette affaire, le CPVP conclut que le consentement approprié n'a pas été obtenu pour la communication de renseignements à Meta (Facebook) dans le cadre de son service de « conversations hors ligne ». L'auteur montre comment le recours continu au consentement implicite soulève de sérieuses questions sur les dispositions relatives au consentement implicite de la *Loi sur la protection de la vie privée des consommateurs* (LPVPC), en opposant ses dispositions relatives au consentement aux protections offertes par le *Règlement général sur la protection des données* (RGPD) de l'Europe, où le consentement équivaut à un consentement explicite. L'auteur affirme que le projet de loi C-27 permet aux entreprises de disposer à la fois des options d'intérêts légitimes et de consentement implicite, ce qui doit être corrigé lors du prochain examen parlementaire du projet de loi C-27.

10. Bennett, Colin J., « 'Privacy Is Like Yoga'- and Other Myths » (*Centre for International Governance Innovation,* 8 février 2023), en ligne à l'adresse : https://www.cigionline.org/articles/privacy-is-like-yoga-and-other-myths/

    L'auteur dénonce plusieurs croyances erronées (souvent défendues par les entreprises qui s'opposent au changement du statu quo) concernant les lois sur la protection des renseignements personnels. Tout d'abord, il remet en question l'idée selon laquelle les lois sur la protection des renseignements personnels doivent toujours trouver un équilibre entre les droits de la personne et les besoins des organisations. Il souligne que la rhétorique constante concernant l'équilibre a permis de normaliser au fil du temps des modèles d'entreprise et des pratiques autrefois considérés comme inacceptables. Puis, il exprime son désaccord avec l'idée que le droit de la protection des renseignements personnels doit toujours être technologiquement neutre. Il affirme que certaines technologies sont intrinsèquement intrusives et répressives et qu'elles ne devraient pas bénéficier d'un traitement neutre. Troisièmement, il conteste les idées reçues sur le RGPD, notamment qu'il est trop intransigeant et prescriptif, qu'il ne repose pas sur des principes flexibles, qu'il est basé uniquement sur les concepts de l'Union européenne et qu'il s'agit d'un régime universel. Il explique que le RGPD est fondé sur des principes et qu'il est le fruit d'un compromis négocié pendant de nombreuses années entre différents intérêts. Enfin, il réfute l'hypothèse selon laquelle le Canada a besoin d'une loi sur la protection des renseignements personnels fondée sur une approche purement canadienne, distincte du

RGPD. Selon lui, l'économie numérique ne change pas de nature au moment de franchir la frontière canadienne et il souligne le fait que de nombreuses multinationales (Apple, Microsoft, etc.) et plus de 140 pays ont été influencés par le RGPD en améliorant leurs normes opérationnelles et en adoptant des lois sur la confidentialité des données, respectivement.

11. Bennett, Colin, One set of privacy rights for Europeans, a lesser one for Canadians? Why the *Canadian consumer privacy protection act and the EU's general data protection regulation should be in alignment*, (20 mai 2021), en ligne à l'adresse : https://www.colinbennett.ca/canadian-privacy/one-set-of-privacy-rights-for-europeans-a-lesser-one-for-canadians-why-the-canadian-consumer-privacy-protection-act-and-the-eus-general-data-protection-regulation-should-be-in-alignment/

    Dans ce blogue, l'auteur explique comment certaines grandes entreprises ou multinationales opérant au Canada cherchent à se conformer au RGPD, et montre comment les Canadiens sont susceptibles de bénéficier d'une norme de protection des renseignements personnels inférieure à celle des Européens, même au sein d'une même entreprise, lorsqu'une entreprise se conforme au RGPD pour les données européennes, mais non pour les données canadiennes. Selon lui, la modernisation d'une telle protection au Canada devrait se conformer au RGPD afin de renforcer les droits des Canadiens et de faire en sorte que ceux-ci ne disposent pas d'un niveau inférieur de protection des renseignements personnels.

12. Bradford, Anu, *The Brussels Effect:* How the European Union Rules the World (2020). Columbia Law School Faculty Books. 232, en ligne à l'adresse : https://scholarship.law.columbia.edu/books/232

    Dans cet ouvrage, l'autrice analyse « l'effet Bruxelles », c'est-à-dire l'influence de la réglementation de l'Union européenne en dehors de l'Europe, la façon dont les sociétés multinationales élèvent leurs normes réglementaires pour se conformer à la législation européenne et comment les normes de l'Union européenne deviennent des normes mondiales.

13. Bremmer, Ian et Mustafa, Suleyman, « *The AI Power Paradox* », (Foreign Affairs, 2023), en ligne (en anglais seulement) : https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox

    Les auteurs soutiennent qu'il faut adopter **une approche « technoprudentialiste » en matière de réglementation de l'IA**, ce qui signifie que l'objectif principal de toute architecture réglementaire mondiale de l'IA devrait être de repérer et d'atténuer les risques pour la stabilité mondiale sans étouffer l'innovation en IA et les possibilités qui en découlent. Les auteurs affirment que l'IA ne peut être régie de la même manière que les technologies antérieures et suggèrent un nouveau cadre de gouvernance adapté au caractère unique de cette technologie. Le « paradoxe du pouvoir de l'IA » est lié à sa nature hyper révolutionnaire, qui rend de plus en plus difficile la résolution de ses défis, y compris en matière de politiques et de dynamique du pouvoir. Les auteurs affirment que

l'utilité de réglementer l'IA dans certains pays est limitée si elle n'est pas réglementée dans d'autres. Ils suggèrent que la gouvernance de l'IA ne saurait présenter de lacune, soulignant les défis que pose la géopolitique actuelle. Le terme « technoprudentialisme » comprend un mandat semblable au rôle macroprudentiel joué par les institutions financières mondiales, dont l'objectif est de déceler et d'atténuer les risques sans compromettre la croissance économique. Les auteurs soutiennent que la gouvernance de l'IA devrait être prudente, agile et inclusive, et ils invitent tous les acteurs nécessaires pour réglementer la pratique à y prendre part. Les auteurs affirment **en outre qu'il devrait y avoir au moins trois régimes de gouvernance de l'IA. L'un serait axé sur la recherche des faits afin de conseiller objectivement les gouvernements et les organismes internationaux (le Groupe d'experts intergouvernemental sur l'évolution du climat est cité comme exemple dont on pourrait s'inspirer). Le second viserait à gérer les tensions entre les grandes puissances de l'IA et à prévenir la prolifération de systèmes d'IA évolués et dangereux. Le dernier pourrait réagir en cas de perturbations dangereuses, comme le fait le Conseil de stabilité financière, qui s'efforce de prévenir l'instabilité mondiale en évaluant les vulnérabilités systémiques et en coordonnant les mesures nécessaires pour y remédier entre les autorités nationales et internationales.**

14. Borrows, John et Lisa Austin, « The Digital Charter Implementation Act ignores Indigenous Data Sovereignty », (commentaire, Université de Toronto, Schwartz Reisman Institute for Technology and Society, le 6 décembre 2022), en ligne : https://srinstitute.utoronto.ca/news/digital-charter-implementation-act-ignores-indigenous-data-sovereignty (en anglais uniquement)

    Les auteurs affirment que le projet de loi C-27 a laissé de côté la voix des communautés autochtones, en notant l'absence de consultation sérieuse avec ces dernières, et qu'on ne s'est pas préoccupé de savoir si le projet de loi C-27 était compatible avec l'obligation du gouvernement fédéral de mettre en œuvre *la Déclaration des Nations unies sur les droits des peuples autochtones* (DNUDPA). Les auteurs notent qu'un certain nombre de dispositions du projet de loi C-27 pourraient être davantage harmonisées avec les lois et les valeurs des peuples autochtones; ils affirment en outre que le paysage des lois canadiennes sur les données ne tient pas compte des principes de l'autodétermination et de l'autonomie gouvernementale des peuples autochtones. Ils soulignent que le projet de loi C-27 permet la divulgation de renseignements anonymisés à l'insu de l'intéressé et sans son consentement « pour une fin socialement bénéfique » sans prévoir d'obligation, lorsque ces renseignements concernent des communautés autochtones, d'obtenir l'autorisation de ces dernières. Plusieurs dispositions du projet de loi C-27 devraient être réexaminées sous l'angle de la souveraineté des données des peuples autochtones.

15. Chen, Chinchih, Carl Benedikt Frey et Giorgio Presidente, *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*, (Oxford Martin School, Université d'Oxford, 6 janvier 2022), en ligne à l'adresse :

https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf

Dans le cadre d'une étude portant sur des entreprises de 61 pays et de 34 secteurs d'activité, les auteurs examinent l'influence de l'introduction du RGPD sur les rendements des entreprises. Ils concluent que les mesures renforcées de protection des données du RGPD et les coûts de mise en conformité afférents ont engendré une baisse de 8 % de la rentabilité des sociétés ciblant les consommateurs européens, avec une incidence exacerbée sur les petites entreprises. Cela dit, les auteurs présentent trois raisons d'interpréter leurs résultats avec prudence : 1) compte tenu du caractère récent du RGPD, les sociétés ont vraisemblablement subi des coûts d'adaptation temporaires sous la forme d'investissements dans de nouvelles technologies conformes au RGPD, susceptibles de diminuer à l'avenir, 2) si le RGPD devient progressivement une norme mondiale, les entreprises ciblant les consommateurs européens seront moins désavantagées au fil du temps, et 3) les répercussions défavorables sur la rentabilité ne tiennent pas compte des effets globaux sur le bien-être, y compris les avantages pour les citoyens concernés par la protection des données. Selon les auteurs, ce dernier point ouvre la voie à d'importantes recherches futures. En outre, ils affirment que « bien que l'on craigne généralement que le RGPD ait freiné l'innovation numérique en Europe, il est tout aussi plausible qu'il l'ait accélérée en incitant les entreprises à mettre au point de nouvelles technologies conformes au RGPD ».

16. Clement, Andrew, « One way we could fund our privacy watchdog », *The Globe and Mail* (éd. de l'Ontario), 3 mars 2023, en ligne à l'adresse : https://www.theglobeandmail.com/business/commentary/article-privacy-commissioner-funding/

    Dans une opinion publiée dans le *Globe and Mail*, le professeur Andrew Clement examine le modèle de financement du « pollueur-payeur » pour les organismes de réglementation de la protection des renseignements personnels[71]. L'auteur oppose les profits faramineux que les grandes entreprises technologiques réalisent grâce à leurs services de publicité ciblée au sous-financement du commissaire à la protection de la vie privée du Canada et propose que les organismes de réglementation soient financés en partie par ceux qui monétisent les données personnelles en vue d'un gain commercial.

17. Clement, Andrew, « The Artificial Intelligence and Data Act needs a reset », *The Hill Times*, 23 novembre 2022, en ligne à l'adresse : https://www.hilltimes.com/story/2022/11/23/the-ai-and-data-act-needs-a-reset/356482/

    L'auteur soutient que la Loi sur l'intelligence artificielle et les données (LIAD) est une législation imparfaite et qu'elle devrait être remaniée. Il cite des exemples d'utilisation récente de l'intelligence artificielle dans les médias sociaux, la technologie de reconnaissance faciale et la collecte massive de données, et souligne l'inquiétude croissante du public face à l'utilisation abusive de systèmes algorithmiques complexes.

[71] Clement, Andrew, « One way we could fund our privacy watchdog », *The Globe and Mail* (éd. de l'Ontario), 3 mars 2023.

Selon lui, la LIAD a été rédigée trop hâtivement, car elle n'a pas suivi le processus normal de consultation publique et a été introduite en même temps que la *Loi pour la mise en œuvre de la Charte numérique*, alors qu'elle aurait dû être dissociée du reste du projet de loi C-27 en vue d'un remaniement en profondeur. Il suggère que le remaniement de la LIAD comprenne une véritable consultation publique, en s'inspirant de la *Loi sur l'intelligence artificielle* de l'Union européenne, en faisant participer les défenseurs des communautés, les chercheurs, les avocats et les représentants des populations à risque. L'auteur affirme que la LIAD devrait faire l'objet d'une surveillance réglementaire indépendante, que la portée des préjudices devrait inclure les préjudices collectifs et pas seulement individuels et que la portée des pratiques algorithmiques pertinentes devrait être élargie pour se concentrer sur la fonction et non sur un ensemble étroit de techniques précises.

18. Cropper, Lorna, « *Data Protection and Digital Information (No. 2) Bill, Take Two* » (Fieldfisher, le 14 avril 2023), en ligne (en anglais seulement) : https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-protection-and-digital-information-no-2-bill

    L'autrice examine l'incidence des modifications proposées dans *la deuxième version du projet de loi sur la protection des données personnelles et de l'information numérique* (le « **projet de loi** »). Elle conclut son analyse en notant que le projet de loi, dans sa forme actuelle, n'aura probablement guère d'écho. Elle souligne que, compte tenu des normes de protection des données remarquablement élevées en vigueur dans l'Union européenne, le gouvernement du Royaume-Uni dispose d'une marge de manœuvre limitée et que, pour cette raison, le projet de loi ne « réinvente pas le domaine de la protection des données ».

19. Comité consultatif de la Convention, « Lignes directrices relatives à la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre des campagnes politiques », (Conseil de l'Europe, 19 novembre 2021), en ligne : https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72

    Le Conseil de l'Europe (**COE**), en particulier le Comité consultatif de la Convention 108, a publié des lignes directrices sur l'utilisation et le traitement des renseignements personnels pour les campagnes politiques. Ces lignes directrices visent à fournir des conseils pratiques aux autorités de protection des données et aux organisations politiques et stipulent que le traitement à des fins de campagnes politiques doit être conforme à la Convention 108 modernisée du COE.

20. Dubois, Elizabeth, « Federal election 2021 : Why we shouldn't always trust 'good' political bots", (19 septembre 2021), en ligne : https://theconversation.com/federal-election-2021-why-we-shouldnt-always-trust-good-political-bots-168137

    Cet article vise à déterminer si les **robots d'IA** (comme **SAMbot d'Areto Labs** et **Polly d'Advanced Symbolics**) et les technologies de surveillance, utilisés et exploités par des acteurs non partisans, ont bénéficié d'une confiance mal placée. Il souligne que ces

technologies représentent des « boîtes noires » et que leurs intrants et leurs activités ne sont pas transparents pour les utilisateurs ou les autres parties intéressées. L'auteur suggère des mesures pour mieux comprendre et évaluer les robots d'IA à l'avenir. Premièrement, **les partis pris inévitables devraient être explicitement reconnus afin que les conclusions puissent être situées et interprétées de façon appropriée**. Deuxièmement, **les processus de formation qui permettent de mettre au point les technologies devraient être mis à la disposition du public**. Troisièmement, il **faut établir des attentes en matière de transparence et de clarté**.

21. Centre de gouvernance de l'information des Premières Nations, « Exploration of the Impact of Canada's Information Management Regime on First Nations Data Sovereignty », (22 août 2022), en ligne : https://fnigc.ca/wp-content/uploads/2022/09/FNIGC_Discussion_Paper_IM_Regime_Data_Sovereignty_EN.pdf (en anglais uniquement)

    Ce document porte sur les conflits entre le régime canadien actuel de gestion de l'information et la souveraineté des données des Premières Nations. Il examine les documents de discussion des gouvernements fédéraux sur la réforme de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* et affirme que pour respecter la souveraineté des Premières Nations en matière de données, il est nécessaire de procéder à un examen systémique du régime canadien de gestion de l'information. Les auteurs du document demandent instamment que soient apportées des modifications de la *Loi sur l'accès à l'information* et aux lois connexes et identifient les domaines à réformer. Le document indique que la souveraineté des données des Premières Nations est un élément de leurs droits inhérents, issus de traités et de la constitution, à l'autodétermination et à l'autonomie, et qu'elle signifie que les données des Premières Nations sont régies par les lois des Premières Nations. Cet élément intègre les principes de PCAP® des Premières Nations – soit la propriété, le contrôle, l'accès et la possession des données. (PCAP® est une marque déposée du Centre de Gouvernance de l'information des Premières Nations). Le document souligne les obstacles systémiques à la souveraineté des données des Premières Nations, notamment la prise de décision unilatérale par la Couronne, un conflit de valeurs et l'imposition d'un régime individualiste, ainsi que la dépendance forcée au droit privé des contrats pour combler une lacune du droit public. Il traite également de la collecte excessive de données et de renseignements des Premières Nations, de la vente par la Couronne à des tiers de l'accès aux données des Premières Nations, du recours par la Couronne à des dispositions imparfaites en matière de consentement pour s'octroyer le pouvoir d'utiliser les données des Premières Nations, de l'utilisation des données des Premières Nations d'une manière qui maintient les stéréotypes négatifs et de la création d'obstacles à l'accès des Premières Nations à leurs données et à leurs renseignements. Le document propose également des suggestions interreliées et multidimensionnelles d'autres travaux d'exploration susceptibles d'améliorer le système à court et à long terme.

22. Centre de gouvernance de l'information des Premières Nations, « *PIPEDA and First Nations: Application and Reform* », (Centre de gouvernance de l'information des

Premières Nations, mars 2023), en ligne (en anglais seulement) : https://fnigc.ca/wp-content/uploads/2023/07/PIPEDA-and-FN-Report_PROOF-002.pdf

Le document examine comment s'appliquent la LPRPDE et les lois provinciales sur la protection de la vie privée dans le secteur privé aux entreprises, aux gouvernements et aux organisations des Premières Nations. Il tient compte de la souveraineté des Premières Nations en matière de données et des principes des Premières Nations du PCAP® dans son analyse de la LPRPDE et de la protection des renseignements personnels. Le document décrit et souligne plusieurs décisions et documents d'orientation importants concernant les conseils de bande. Il examine le projet de loi C-27 et utilise un aperçu de la *Déclaration des Nations Unies sur les droits des peuples autochtones* (DNUDPA) pour critiquer et préparer la réforme du droit canadien en matière de vie privée dans le secteur privé du point de vue de la souveraineté des Premières Nations en matière de données.

23. Gunst, Simona et Ferdi De Ville, « The Brussels Effect: How the GDPR Conquered Silicon Valley », *European Foreign Affairs Review*, vol. 26, nº 3 (2021), p. 437 à 458, en ligne à l'adresse : https://doi.org/10.54648/eerr2021036 (sous le verrou d'accès payant)

Les auteurs examinent si l'effet Bruxelles établit un lien de causalité entre le California Consumer Privacy Act (CCPA) et le RGPD sur la base de trois séries de preuves : les politiques de protection des renseignements personnels d'Apple, de Google et de Facebook, les démarches de lobbying et l'utilisation par le gouvernement californien d'arguments liés à l'effet Bruxelles lors de la rédaction du CCPA. Ils concluent que l'effet Bruxelles a joué un rôle dans l'adoption du CCPA et que l'impact de celui-ci varie en fonction de la disposition du RGPD.

24. Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique en anglais, Office of the Information & Privacy Commissioner for British Columbia ou OIPC) « Guidance Document, Political Campaign Activity », (août 2022), en ligne https://www.oipc.bc.ca/guidance-documents/3700

Ce document d'orientation du Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique (OIPC) présente les meilleures pratiques pour les organisations politiques et leur traitement des renseignements personnels dans le cadre du processus de campagne. Il est particulièrement important, car **la *Personal Information Protection Act* (PIPA) de la Colombie-Britannique s'applique à la collecte, à l'utilisation et à la communication de « renseignements personnels » par les partis politiques de la Colombie-Britannique.** Ce document examine comment les organisations politiques peuvent recueillir et utiliser des renseignements personnels, comment les organisations doivent informer les personnes concernant la collecte, ce qui constitue un objectif raisonnable et comment les organisations peuvent mettre en œuvre de solides programmes de gestion de la confidentialité. Il complète le *Political Campaign Activity Code of Practice* de l'OIPC.

25. Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, « Political Campaign Activity Code of Practice », (mars 2021), en ligne : https://www.oipc.bc.ca/guidance-documents/3653

    Ce code, rédigé par l'OIPC et Elections BC, vise à établir des règles de base volontaires pour des règles du jeu équitables entre les campagnes électorales et à équilibrer le rôle des partis politiques avec la protection de la vie privée des personnes. Il demande aux partis politiques de s'engager à adopter dix pratiques électorales équitables, allant de l'obtention d'un consentement valable à l'application de mesures de protection de la vie privée adéquates par l'entremise d'un programme de gestion de la vie privée.

26. Commissariat à la protection de la vie privée du Canada, « Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-27, la Loi de 2020 sur la mise en œuvre de la Charte du numérique », avril 2023, en ligne : https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_indu_c27_2304/

    Dans le mémoire sur le projet de loi C-27 présenté par le CPVP au INDU, le commissaire à la protection de la vie privée du Canada, Philippe Dufresne, estime que ce texte est un « pas dans la bonne direction », en ajoutant cependant qu'il « peut et doit être amélioré davantage ». Le mémoire du CPVP contient 15 recommandations assorties de suggestions de modifications à apporter au projet de loi C-27, ainsi qu'une annexe où sont énumérées d'autres façons d'améliorer ce texte qui s'appuient sur les recommandations antérieures du CPVP au sujet de l'ancien projet de loi C-11. La recommandation n° 1 du CPVP affirme que la protection de la vie privée doit être reconnue comme un droit fondamental, tant dans le préambule que dans l'article 5 de la LPVPC. Le CPVP suggère que ce préambule amélioré soit intégré non seulement à la LPVPC, mais aussi à la LTPRPD et à la LIAD. La recommandation n° 2 du CPVP vise à protéger la vie privée des enfants et l'intérêt supérieur de l'enfant. Le CPVP recommande que soit modifié le préambule du projet de loi C-27 afin d'y inclure une mention prévoyant explicitement que le traitement des renseignements personnels devrait protéger la vie privée des enfants et l'intérêt supérieur de l'enfant. Parmi les autres recommandations clés du CPVP, mentionnons : élargir de la liste des contraventions pouvant faire l'objet de sanctions pécuniaires pour y inclure, au minimum, les contraventions aux fins acceptables; offrir une plus grande souplesse pour l'utilisation des accords de conformité volontaires en vue de régler les affaires sans avoir recours à des processus litigieux; établir une culture de protection de la vie privée en exigeant des organisations qu'elles intègrent la protection de la vie privée dès la conception des produits et des services et qu'elles mènent des évaluations des facteurs relatifs à la vie

privée pour les initiatives à risque élevé; prévoir un droit de procéder à l'élimination des renseignements personnels même si une politique de conservation est en vigueur.

27. Commissariat à la protection de la vie privée du Canada, Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-11, la Loi de 2020 sur la mise en œuvre de la Charte du numérique, mai 2021, en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_ethi_c11_2105/

Dans ce mémoire historique, le commissaire à la protection de la vie privée a déclaré que l'ancien projet de loi C-11 représentait un recul global en matière de protection de la vie privée et qu'il nécessitait des changements importants sous trois thèmes principaux : 1) une meilleure articulation du poids des droits à la vie privée et des intérêts commerciaux, 2) des droits et obligations spécifiques, et 3) l'accès à des recours rapides et efficaces et le rôle du CPVP. Le mémoire recommande plus de 65 amendements détaillés au projet de loi C-11, notamment que la législation fédérale sur la protection des renseignements personnels dans le secteur privé fasse de la protection des renseignements personnels un droit fondamental de la personne.

Voir l'article connexe suivant

Scassa, Teresa, « Bill C-11's Treatment of Cross-Border Transfers of Personal Information », (Université d'Ottawa, mai 2021), en ligne : https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/

Le document, commandé par le Commissariat à la protection de la vie privée du Canada (CPVP), énonce les principaux éléments à prendre en considération dans un cadre de protection de la vie privée qui traite des flux de données transfrontaliers. L'auteur examine les dispositions du projet de loi C-11, plus précisément la LPVPC, et fournit une analyse critique de la mesure dans laquelle ses dispositions protègent la vie privée. L'auteure compare également les dispositions de la LPVPC aux mesures offertes par des administrations comparables et formule douze recommandations sur la façon d'améliorer la LPVPC dans le projet de loi C-11 afin de mieux protéger la vie privée dans le contexte des transferts internationaux. Plus précisément, l'auteur recommande que la LPVPC comprenne une disposition spéciale pour traiter des flux de données transfrontaliers. Plusieurs des recommandations indiquent également comment la LPVPC pourrait être modifiée, par exemple, afin d'avoir des dispositions claires et non ambiguës en ce qui concerne le contexte transfrontalier. Le mémoire du CPVP sur le projet de loi C-11 (mentionné ci-dessus) s'est fortement appuyé sur ce document pour formuler ses recommandations sur les flux de données transfrontaliers.

28. Commissariat à la protection de la vie privée du Canada, « Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2022-2023 » (mars 2023), en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-

commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2023/por_ca_2022-23/

Le sondage du CPVP révèle **que les Canadiens sont hautement préoccupés par la protection de leur vie privée, 93 % d'entre eux ayant exprimé avoir de telles préoccupation**s. Le sondage a également révélé que le nombre de Canadiens qui croyaient que les entreprises respectaient leurs droits à la vie privée avait diminué. À ce chapitre, ce sont les entreprises de médias sociaux dont les Canadiens se méfiaient le plus. Seulement un Canadien sur dix fait confiance aux entreprises de médias sociaux pour protéger ses renseignements personnels.

29. Commissariat à la protection de la vie privée du Canada, « Sondage auprès des Canadiens à propos des questions entourant la protection de la vie privée, 2020-21 (mars 2021), en ligne : https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/

Ce sondage bisannuel commandé par le commissaire à la protection de la vie privée du Canada et mené par Phoenix Strategic Perspectives Inc. vise à mieux comprendre la mesure dans laquelle les Canadiens sont au courant, comprennent et perçoivent les enjeux liés à la protection de la vie privée. **Le sondage indique que les Canadiens ne sont que légèrement plus préoccupés par la sécurité que par la protection de la vie privée (89 % à 87 %). De plus, il estime que les préoccupations des Canadiens au sujet de l'utilisation des renseignements personnels (RP) dans le secteur public ne l'emportent pas sur les préoccupations au sujet de l'utilisation des renseignements personnels dans le secteur privé.** Les Canadiens se sentent un peu plus informés sur la façon dont leurs RP sont gérés par le secteur public (écart de 3 %) et ils sont beaucoup plus confiants que le gouvernement fédéral respecte leurs droits à la vie privée comparativement aux entreprises privées (écart de 18 %).

30. Parson, Christopher et Amanda Cutinha, « Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law », Citizen Lab, rapport de recherche n° 161, (22 novembre 2022), en ligne : https://citizenlab.ca/wp-content/uploads/2022/11/Report161-Minding-Your-Business.pdf (en anglais uniquement)

Les auteurs affirment que le projet de loi C-27 ne corrige pas les lacunes actuelles de la LPRPDE et proposent de lui apporter 19 modifications législatives qui amélioreraient la responsabilisation des entreprises et des gouvernements en matière de collecte, d'utilisation et de communication de renseignements sur les résidents et les collectivités du Canada, y compris les renseignements dépersonnalisés. En particulier, les auteurs évaluent de manière critique la pratique gouvernementale de collecte des renseignements sur la mobilité à des fins socialement bénéfiques ainsi que la capacité des organisations privées de recueillir et d'utiliser des renseignements personnels sans obtenir au préalable le consentement des personnes ou sans les informer de leurs activités commerciales. Le rapport se compose de cinq parties : La partie 1 présente un historique des principaux enjeux en matière de protection des renseignements personnels qui ont été associés à la

collecte de données sur la mobilité pendant la pandémie de COVID-19; la partie 2 résume et présente les principales constatations des séances du comité ETHI sur la façon dont le gouvernement fédéral a obtenu et utilisé les données sur la mobilité pendant la pandémie de COVID-19; la partie 3 évalue la légalité de la façon dont les données sur la mobilité peuvent être et ont été obtenues et utilisées par le gouvernement fédéral; la partie 4 présente six lacunes thématiques dans la législation canadienne sur la protection des renseignements personnels : 1. La LPRPDE ne protège pas de manière adéquate les intérêts liés à la vie privée menacés dans les situations de dépersonnalisation et d'agrégation des données, malgré les risques associés à la ré-identification; 2. La LPRPDE ne comporte aucune disposition exigeant que les personnes soient informées de la façon dont leurs données sont dépersonnalisées ou utilisées à des fins secondaires; 3. La LPRPDE ne permet pas aux particuliers ou aux collectivités de prévenir de manière suffisante les effets préjudiciables du partage de données avec le gouvernement; 4. La LPRPDE ne prévoit pas de contrôles et de contrepoids suffisants pour garantir l'obtention d'un consentement valable à la collecte, à l'utilisation ou à la divulgation des données dépersonnalisées; 5. **La LPRPDE ne tient pas compte de la souveraineté des données des peuples autochtones ni des principes de souveraineté des peuples autochtones énoncés dans la *Déclaration des Nations Unies sur les droits des peuples autochtones*, qui a été adoptée par le Canada**; et 6. De manière générale, la LPRPDE ne prévoit pas de mécanismes d'application suffisants. La partie 5 du rapport analyse les articles pertinents de la LPVPC et soutient qu'elle ne comble pas les lacunes de la LPRPDE et qu'elle pose plutôt un certain nombre de problèmes.

31. Scassa, Teresa, « *Regulating AI in Canada : a critical look at the proposed Artificial Intelligence and Data Act* », (La Revue du Barreau canadien, 2023, vol 101, no. 1), en ligne (en anglais seulement à l'exception d'un sommaire) : https://cbr.cba.org/index.php/cbr/article/view/4817/4539

L'autrice procède à une analyse de la LIAD et du contexte dans lequel elle a été déposée, et formule des recommandations afin de l'améliorer. L'autrice révèle plusieurs lacunes dans la LIAD, notamment le fait qu'elle met l'accent sur les systèmes d'IA à forte incidence sans pour autant définir le terme « forte incidence ». Selon l'autrice, la caractéristique frappante de la LIAD, c'est qu'il reste tant à définir dans les règlements qu'elle semble dépourvue de contenu substantiel et être un « chèque en blanc » réglementaire. L'autrice examine en quoi consiste une réglementation « agile » et constate que l'agilité ne consiste pas à s'appuyer sur la réglementation, mais plutôt à appuyer les organismes de réglementation afin que leur pratique réglementaire soit plus souple, mieux adaptée et davantage axée sur les données.

Elle se penche également sur les initiatives de gouvernance de l'IA à l'échelle internationale, y compris sur les approches fondées sur le risque adoptées dans l'UE dans le contexte de la *Loi sur l'IA de l'UE*, ainsi que sur le cadre de gestion des risques de l'IA des États-Unis dont l'auteur est le *National Institute of Standards and Technology*. L'autrice souligne qu'en vertu de la LIAD, le ministre et le commissaire aux données sont responsables de l'application de la LIAD, mais que les deux postes relèvent du ministère chargé du soutien à l'innovation et au développement économique, ce qui

soulève des questions sur leur indépendance. La LIAD exclut ou omet également les groupes et les collectivités, ne mettant l'accent que sur les personnes et uniquement sur les préjudices quantifiables. L'autrice critique le gouvernement pour l'absence de consultation sur la LIAD; elle conclut que la LIAD devrait être supprimée et recommande le lancement d'une consultation en bonne et due forme sur l'IA.

32. Scassa, Teresa, « Canada's Draft AI Legislation Needs Important Revisions », (Centre for International Governance Innovation, août 2023), en ligne : https://www.cigionline.org/articles/canadas-draft-ai-legislation-needs-important-revisions/?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=ukraines-reconstruction-can-inform-the-wests-digital-transformation

    L'autrice soutient que la technologie de l'IA évolue si rapidement qu'elle nécessite l'intervention d'une réglementation « agile », mais que la LIAD est une loi précipitée et problématique. Elle décrit en détail cinq critiques de la LIAD, affirmant qu'une révision permettrait de répondre entièrement à celles-ci. Elle affirme que, même si le gouvernement décrit son approche en matière de réglementation de l'IA comme une réglementation « agile », la LIAD prévoit qu'une grande partie de la loi sera déclinée à travers des règlements qui ne seront pas « agiles », car les règlements sont souvent élaborés plus lentement que prévu et, dans certains cas, ne voient jamais le jour. L'autrice fait remarquer que la LIAD vise à réglementer les systèmes d'IA à fort impact, mais que la définition de « fort impact » reste à établir dans les règlements futurs. La LIAD ne désigne pas d'organisme de réglementation indépendant et conçoit le préjudice de façon restreinte, omettant notamment la discrimination systémique ou le préjudice environnemental et limitant essentiellement sa définition actuelle du « préjudice » à des préjudices quantifiables pour les personnes. L'autrice critique également l'absence de vision globale du gouvernement en matière de gouvernance et de réglementation de l'IA.

33. Scassa, Teresa, « Proposed Data Privacy Law Favour Industry Over Individuals », (Toronto Star, 7 octobre 2022), en ligne : https://www.thestar.com/opinion/contributors/2022/10/07/proposed-data-privacy-law-favour-industry-over-individuals.html

    L'auteure utilise la métaphore de Blanche DuBois, tirée de « Un tramway nommé Desire », pour critiquer le projet de **loi C-27**, à savoir qu'il **facilite l'utilisation des données sans prévoir de protections adéquates, ce qui ne renforce pas la confiance dans les pratiques relatives aux données,** créant un risque d'exploitation découlant de la dépendance à « la gentillesse d'étrangers ».

Les articles de blogues suivants, rédigés par Docteure Teresa Scassa, sont une série de publications sur le projet de loi C-27, qui vise à réformer la législation canadienne sur la protection de la vie privée dans le secteur privé. Ces publications examinent certaines dispositions de la Loi sur la protection de la vie privée des consommateurs (LPVPC) et de la Loi sur l'intelligence artificielle et les données (LIAD), et présentent des observations et une analyse de l'incidence de la loi proposée.

34. Scassa, Teresa, « Bill C-27's Take on Consent : A Mixed Review », (4 juillet 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=355:bill-c-27%E2%80%99s-take-on-consent-a-mixed-review&Itemid=80

    Ce document examine le projet de loi C-27 et le compare à l'ancien projet de loi C-11, l'ancien projet de loi sur la modernisation de la protection de la vie privée, qui est mort au Feuilleton avant les dernières élections fédérales de 2021. Plus précisément, la publication analyse la différence entre les dispositions sur le consentement et ce qui est modifié et nouveau dans le projet de loi C-27. L'auteur fait remarquer que, même si le projet de loi C-27 prévoit une série de révisions pour répondre aux préoccupations des défenseurs de la vie privée et de l'industrie, il n'**y a pas grand-chose qui change par rapport à l'ancien projet de loi C-11**.

35. Scassa, Teresa, « Anonymization and De-identification in Bill C-27 », (4 juillet 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80

    Le présent document examine les dispositions du projet de loi C-27 relatives à l'anonymisation et à la dépersonnalisation, en les comparant à celles de l'ancien projet de loi C-11, la *Loi 25*, et au régime de la LPRPDE. L'auteur affirme que les modifications proposées dans le projet de loi 27 reflètent le pouvoir du lobbying de l'industrie, puisqu'il existe deux définitions distinctes des données anonymisées et dépersonnalisées, et que les organisations seront heureuses d'avoir une catégorie distincte de données « anonymisées », ce qui dépasse la portée de la loi. L'auteur examine également la définition du terme « dépersonnaliser » énoncée dans le projet de loi C-27, qui renvoie à la modification des données de manière à ce que les personnes ne puissent être identifiées *directement*, ce qui pourrait entraîner l'utilisation des données à l'insu de l'intéressé ou sans son consentement dans certaines circonstances, même si certaines personnes pourraient encore être identifiées à partir de ces ensembles de données. L'auteure constate que le projet de **loi C-27 a réduit la définition de la dépersonnalisation par rapport à l'ancien projet de loi C-11 et n'a fourni que peu ou pas d'indications au-delà des « pratiques exemplaires généralement reconnues » pour traiter de l'anonymisation**.

36. Scassa, Teresa, « Statutory MadLibs – Canada's Artificial Intelligence and Data Act », (20 juillet 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=359:statutory-

madlibs-%E2%80%93-canada%E2%80%99s-artificial-intelligence-and-data-act&Itemid=80

Ce poste utilise l'utilisation d'un MadLib pour démontrer **les nombreux éléments laissés à la réglementation dans la LIAD**.

37. Scassa, Teresa, « Bill C-27 and the erasable right of erasure », (18 juillet 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=358:bill-c-27-and-the-erasable-right-of-erasure&Itemid=80

Cette publication explique le **droit d'effacer** - le droit pour les individus de demander à une organisation d'éliminer des renseignements personnels qu'elle détient à leur sujet - prévu dans le projet de loi C-27. Teresa Scassa note que le droit ne s'applique que dans trois circonstances et met en évidence les exceptions potentiellement problématiques, notamment i) lorsque la suppression des renseignements personnels aurait un impact négatif indu sur la fourniture continue d'un produit ou d'un service, ii) lorsque les renseignements personnels doivent être supprimés conformément à la politique de conservation des renseignements personnels d'une organisation, et iii) lorsque les demandes de suppression sont « vexatoires ou faites de mauvaise foi ». Elle estime que **l'équilibre dans le projet de loi C-27 favorise la libre circulation des données personnelles plutôt que la protection de la vie privée**. La publication conclut qu'un droit destiné à donner plus de contrôle aux personnes ne fait que fournir aux organisations de nombreuses exceptions pour s'en soustraire.

38. Scassa, Teresa, « Data Sharing for Public Good : Does Bill C-27 Reflect Lessons Learned from Past Public Outcry? », (11 juillet 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=357:data-sharing-for-public-good-does-bill-c-27-reflect-lessons-learned-from-past-public-outcry?&Itemid=80

Cette publication met en lumière les dispositions du projet de loi C-27, conçues pour répondre aux besoins du gouvernement et de l'industrie des données commerciales en ce qui concerne l'accès aux données personnelles entre les mains du secteur privé. On y souligne la portée élargie de la disposition du projet de loi C-27 concernant les statistiques et la recherche (art. 35), ce qui pourrait permettre de façon problématique des recherches sur le marché et le profil des électeurs en raison de la suppression du terme « érudit ». Des préoccupations semblables au sujet de la portée accompagnent l'article 39, qui porte sur la communication de renseignements personnels dépersonnalisés à des « fins bénéfiques sur le plan social ». Le message identifie des garde-fous importants introduits dans la *Loi 25* du Québec et suggère que ces pratiques, y compris l'exigence d'une évaluation des facteurs relatifs à la vie privée, soient incluses dans le projet de loi C-27. Il conclut que le projet de **loi C-27 facilite l'utilisation sans protéger adéquatement la vie privée**, ce qui est une approche cynique compte tenu du manque de confiance envers le gouvernement découlant des récentes controverses entourant le partage de données entre Statistique Canada et l'ASPC.

39. Scassa, Teresa, « Bill C-27 and Children's Privacy », (25 juillet 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=360:bill-c-27-and-children%E2%80%99s-privacy&Itemid=80

    Dans cette publication, on dit que le projet de loi C-27 répond modestement aux préoccupations des défenseurs de la protection de la vie privée des enfants. On y souligne que les préoccupations constitutionnelles concernant l'âge de la majorité peuvent limiter une réponse plus ferme. L'auteure laisse entendre que la caractérisation explicite des données des mineurs comme « sensibles » et l'exclusion des restrictions au droit d'effacement pour les mineurs représentent une amélioration par rapport à la LPRPDE et à l'ancien projet de loi C-11. Elle conclut que le projet de **loi C-27 améliore dans une certaine mesure les droits des mineurs en matière de protection des données**.

40. Scassa, Teresa, « Bill C-27 and a human rights-based approach to data collection », (2 août 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=361:bill-c-27-and-a-human-rights-based-approach-to-data-protection&Itemid=80

    Cette publication souligne que la vie privée est un droit de la personne, reconnu dans les instruments internationaux et doté d'un statut quasi constitutionnel par la Cour suprême du Canada. On y explique que, contrairement au projet de loi C-11, le projet de loi C-27 mentionne le fondement de la protection de la vie privée en matière de droits de la personne dans son préambule, mais considère qu'il s'agit simplement d'un facteur à prendre en compte, en plus du fardeau de l'innovation et de la réglementation. Le message met en évidence les effets potentiels des disparités entre les approches adoptées dans le projet de loi C-27 et le RGPD de l'UE et la *Loi 25* du Québec. L'auteure conclut que la protection de la vie **privée en tant que droit de la personne devrait être le point de départ des lois canadiennes sur la protection de la vie privée et que, même si l'innovation est bonne, elle ne peut pas se faire au détriment des droits de la personne**.

41. Scassa, Teresa, « Canada's Proposed AI and Data Act - Purpose and Application », (8 août 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=362:canadas-proposed-ai--data-act-purpose-and-application&Itemid=80

    Cette publication examine la portée de la LIAD, expliquant certains de ses défis constitutionnels (répartition des pouvoirs), tels qu'on les trouve dans le double objectif de la LIAD. On y indique que la LIAD ne s'applique pas aux institutions fédérales et à certaines institutions de la défense nationale, et **qu'il n'y a aucune raison pour que les utilisations de l'IA par la défense nationale non militaire ne soient pas assujetties à une gouvernance**. On y **souligne également les limites de la LIAD et on critique la quantité d'informations qui reste à déterminer par la réglementation, en particulier la définition de « système à fort impact** ».

42. Scassa, Teresa, « Regulated Activities and Data under Bill C-27's AI and Data Act », (15 août 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=363:regulated-activities-and-data-under-bill-c-27s-ai-and-data-act&Itemid=80

    Cette publication examine les activités de la LIAD et les données qui seront soumises à la gouvernance en vertu de la LIAD. On y dit que la LIAD régit deux catégories d'« activités réglementées », à condition qu'elles soient exercées « dans le cadre du commerce international ou interprovincial ». On y explique comment ces activités sont présentées en termes généraux et comment les obligations de la LIAD ne s'appliquent pas universellement à tous ceux qui sont engagés dans l'industrie de l'IA. L'auteure note que, **pour de nombreuses dispositions, les détails de ce qui est réellement requis dépendront des réglementations qui doivent encore être rédigées**. Elle met également en lumière une comparaison du régime de gouvernance et de surveillance proposé dans la LPVPC et la LIAD, soulignant que la LPVPC assure une surveillance par un mandataire indépendant du Parlement, contrairement à la LIAD.

43. Scassa, Teresa, « The Unduly Narrow Scope for « Harm » and « Biased Output » Under the AIDA », (22 août 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=364:the-unduly-narrow-scope-for-harm-and-biased-output-under-the-aida&Itemid=80

    Cette publication **examine la portée trop étroite des termes « préjudice » et « production biaisée » en vertu de la LIAD.** L'auteure souligne que la notion de préjudice est importante pour le cadre de la LIAD et décrit certaines obligations pour les personnes responsables des systèmes d'IA à fort impact, comme l'obligation de cerner, d'évaluer et d'atténuer les risques de préjudice ou de produits biaisés, et d'aviser le ministre responsable dans certaines circonstances. Elle explique également les fonctions de surveillance et d'application de la LIAD, y compris les pouvoirs accordés au ministre en vertu de la LIAD. On y analyse l'utilisation du terme « individu » dans les définitions de « préjudice » afin de démontrer les limites de la LIAD et on examine la différence entre l'utilisation du terme « préjudice » et « produit biaisé » dans le cadre de la LIAD, en soulignant que la définition de « préjudice » ne comprend pas le terme « produit biaisé ».

44. Scassa, Teresa, « Oversight & Enforcement Under Canada's Proposed AI and Data Act », (29 août 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=365:oversight-and-enforcement-under-canadas-proposed-ai-and-data-act&Itemid=80

    Cette publication explique que le projet de loi C-27 crée de nouvelles obligations pour les personnes responsables des systèmes d'IA, en particulier les systèmes à fort impact, ainsi que pour celles qui traitent ou rendent disponibles des données anonymisées pour utilisation dans les systèmes d'IA. L'auteure souligne que la LPVPC confère une série de nouveaux pouvoirs d'exécution, notamment le pouvoir de rendre des ordonnances et

d'imposer des sanctions administratives pécuniaires (SAP) en cas de non-conformité. L'auteure examine le « mordant » de la LIAD, soulignant que la LIAD **elle-même ne prévoit aucun mécanisme permettant aux personnes de déposer des plaintes concernant les préjudices qu'elles croient avoir subis, et qu'il ne prévoit aucune disposition pour l'examen des plaintes**. Le message critique également **le manque d'indépendance par rapport au gouvernement dans la surveillance de la LIAD** et analyse les différentes voies d'imposition de sanctions administratives pécuniaires ou d'amendes. La publication se termine par une critique du **manque de détails importants trouvés dans la LIAD concernant son système de surveillance et d'application.**

45. Scassa, Teresa, « Regulating AI in Canada - The Federal Government and the AIDA », (11 octobre 2022), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=366:regulating-ai-in-canada-the-federal-government-and-the-aida&Itemid=80

    Cette publication examine le pouvoir constitutionnel du gouvernement fédéral d'adopter la LIAD. Plus précisément, l'auteure se demande si le gouvernement fédéral a compétence pour réglementer l'IA. La publication se penche également sur d'autres instruments juridiques de l'IA dans l'Union européenne et aux États-Unis, ainsi que sur d'autres cadres politiques pour l'utilisation de l'IA.

46. Scassa, Teresa, « Explaining the AI and Data Act » (21 mars 2023), en ligne :

    https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=369:explaining-the-ai-and-data-act&Itemid=80 (en anglais uniquement)

    Dans cette publication, l'auteure se demande si le document complémentaire d'ISDE du 13 mars 2023 sur la LIAD répond aux nombreuses critiques du projet de loi tel qu'il a été déposé par le gouvernement le 16 juin 2022. L'auteure conclut que le document d'ISDE n'aborde pas ces critiques et qu'une refonte substantielle de la LIAD s'avère nécessaire.

47. Scassa, Teresa, « Comparing the UK's proposal for AI governance to Canada's AI bil » (11 avril 2023), en ligne : http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=370:comparing-the-uks-proposal-for-ai-governance-to-canadas-ai-bill&Itemid=80 (en anglais uniquement)

    L'auteure compare la LIAD au document de consultation du Royaume-Uni, qui sollicite des commentaires sur la proposition de réglementation de l'IA par le Royaume-Uni, et constate que les deux textes sont très différents. Par exemple, la LIAD réglemente l'IA à incidence élevée, qui reste à être définie dans les règlements de la LIAD, tout comme d'autres éléments essentiels. La LIAD prévoit également que le ministre de l'Innovation est généralement responsable de sa surveillance et de son application. L'auteure note que plutôt que de créer un nouveau texte législatif et/ou une nouvelle autorité réglementaire, la proposition britannique énonce cinq principes pour un développement et une utilisation responsables de l'IA. Au Royaume-Uni, les organismes de réglementation existants

seront encouragés à réglementer l'IA selon ces principes en fonction de leurs sphères de compétence et, au besoin, elles seront expressément habilitées à le faire. Parmi les organismes de réglementation qui participeront à ce cadre figurent le Commissariat à l'information et les organismes de réglementation chargés des droits de la personne, de la protection des consommateurs, des produits de soins de santé et des appareils médicaux, et du droit de la concurrence. Le schéma du Royaume-Uni reconnaît également qu'une entité gouvernementale pourrait être nécessaire pour exécuter certaines fonctions de soutien centralisées. Ces fonctions pourraient être notamment le suivi et l'évaluation, l'éducation et la sensibilisation, l'interopérabilité internationale, l'analyse de l'horizon et des lacunes, et le soutien aux bancs d'essai et aux bacs à sable. Selon l'auteure, même si le gouvernement fédéral du Canada décrit son approche en matière de réglementation de l'IA comme une réglementation « agile », celle du Royaume-Uni se rapproche beaucoup plus de ce concept.

48. Scassa Teresa, « Federal Court Dismisses Application for an Order against Facebook - and Raises Some Issues for PIPEDA Reform », (17 avril 2023), en ligne : https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=371:federal-court-dismisses-application-for-an-order-against-facebook-and-raises-some-issues-for-pipeda-reform&Itemid=80 (en anglais uniquement)

Ce billet traite de l'action intentée devant la Cour fédérale du Canada par le Commissaire à la protection de la vie privée du Canada à l'encontre de Facebook, en lien avec le scandale Cambridge Analytica. L'auteure affirme que la Cour fédérale a rejeté la demande du Commissaire à la protection de la vie privée en grande partie en raison de l'absence de preuve établissant que Facebook n'avait pas respecté ses obligations en vertu de la LPRPDE de protéger les renseignements personnels de ses utilisateurs. L'auteure affirme que la Cour a réprimandé le Commissaire pour son processus de collecte d'éléments de preuve, y compris pour n'avoir pas utilisé les pouvoirs que lui confère la loi pour ordonner la production de la preuve. Elle se penche également sur le caractère profondément troublant de certains aspects de la décision pour ceux qui se préoccupent de la protection de la vie privée, comme l'abandon de la dimension normative du concept de l'attente raisonnable en matière de vie privée. **L'auteure affirme également que certains aspects de la décision devraient sonner l'alarme en ce qui concerne le projet de loi C-27, soulignant, par exemple, que dans le cas de la communication à des tiers à des fins socialement bénéfiques, la loi devrait prévoir des mesures de sauvegarde et qu'une approche fondée sur les droits de la personne pourrait fournir un solide filet de sécurité lorsqu'il faut tenir compte des intérêts commerciaux.** L'auteure conclut en soulignant qu'une mauvaise loi peut engendrer de mauvaises décisions judiciaires et que le défi sera de veiller à ce que le projet de loi C-27 ne reproduise pas ou n'amplifie pas les lacunes de la LPRPDE.

49. Solove, Daniel J., « The Myth of the Privacy Paradox », (George Washington University Law School, 2020), en ligne : https://scholarship.law.gwu.edu/faculty_publications/1482/

    L'auteur examine le phénomène du « paradoxe de la protection de la vie privée », où les gens disent accorder une grande importance à la protection de la vie privée, mais, dans leur comportement, renoncent à leurs données personnelles pour très peu en échange ou omettent d'utiliser des mesures pour protéger leur vie privée. L'auteur **déconstruit et critique le paradoxe de la protection de la vie privée et les arguments présentés à ce sujet.**

50. Travers Smith LLP, « Data Protection and Digital Information (no. 2) Bill » (17 mars 2023), en ligne : https://www.traverssmith.com/knowledge/knowledge-container/data-protection-and-digital-information-no-2-bill/

    Le texte examine les principales réformes pour la protection des données personnelles proposées dans *la deuxième version du projet de loi sur la protection des données personnelles et de l'information numérique au Royaume-Uni* (le « **projet de loi** »). L'auteur estime que le projet de loi pourrait être « une sorte de pétard mouillé après la rhétorique d'octobre » et estime que « le risque que ces réformes aient un impact sur l'adéquation du Royaume-Uni semble faible ». Il souligne également qu'on s'attend à ce que les organisations qui répondent déjà aux exigences du RGPD actuel du Royaume-Uni soient également conformes aux dispositions du projet de loi.

51. Tessono, Christelle et Yuan Stevens, Momin M. Malik, Sonja Solomun, Supriya Dwivedi et Sam Andrey, « AI Oversight, Accountability and Protecting Human Rights: Comments on Canada's Proposed Artificial Intelligence and Data Act » (publié en collaboration par le Cybersecure Policy Exchange de l'Université métropolitaine de Toronto, le Centre pour les médias, la technologie et la démocratie de l'Université McGill et le Center for Information Technology Policy de l'Université Princeton, novembre 2022), en ligne : https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/63614c030e02403d54fce254/1667320848453/AIDACommentary.pdf (en anglais uniquement)

    Ce rapport a été publié en collaboration par des chercheurs du Cybersecure Policy Exchange de l'Université métropolitaine de Toronto, du Centre pour les médias, la technologie et la démocratie de l'Université McGill et du Center for Information Technology Policy de l'Université Princeton. Les auteurs formulent plusieurs recommandations afin d'améliorer les principales préoccupations liées à la LIAD. **Ces recommandations sont les suivantes : (1)** organiser des consultations publiques adéquates sur la LIAD avec les défenseurs des communautés, les chercheurs, les avocats et les groupes représentant les intérêts des PANDC, des 2SLGBTQIA+, des populations économiquement défavorisées, des personnes handicapées et d'autres populations en quête d'équité; **(2)** que la LIAD soit effectivement réglementée par un agent indépendant du Parlement et dotée d'un tribunal indépendant chargé d'administrer les sanctions en cas d'infraction; **(3)** que la LIAD s'applique aux institutions gouvernementales; que la définition de l'IA soit neutre sur le plan technologique et à l'épreuve de l'avenir, par

exemple, en mettant l'accent sur les applications de l'IA plutôt que sur les techniques, et que la définition de l'IA soit uniforme dans l'ensemble de la LPVPC et de la LIAD; **(4)** que le projet de loi C-27 traite de façon exhaustive des répercussions des systèmes d'intelligence artificielle sur les droits de la personne, par exemple en interdisant le traitement de données biométriques comme la reconnaissance faciale, sous réserve d'un nombre limité d'exceptions; **(5)** que des recours soient disponibles afin de protéger les droits fondamentaux, comme le droit de s'opposer au traitement automatisé des données personnelles et le droit d'interjeter appel des décisions relatives à l'IA; **(6)** que certaines utilisations de l'IA soient interdites, par exemple, les utilisations qui exploitent des groupes vulnérables ou qui comprennent l'établissement de cotes sociales; et que le projet de loi C-27 et la LIAD prévoient expressément des niveaux élevés de protection par défaut pour les enfants.

52. La Maison-Blanche (États-Unis), « Blueprint for an AI Bill of Rights », octobre 2022, en ligne : https://www.whitehouse.gov/ostp/ai-bill-of-rights/

Le *plan directeur pour une Déclaration des droits de l'IA* contient cinq principes directeurs pour la conception, l'utilisation et le déploiement de systèmes automatisés, qui sont susceptibles d'avoir une incidence significative sur les droits, les possibilités ou l'accès du public américain à des ressources ou à des services essentiels. La Maison-Blanche affirme que le *plan directeur pour une Déclaration des droits de l'IA* a été élaboré à la suite de vastes consultations auprès du public américain, et qu'il consiste en un plan directeur pour la construction et le déploiement de systèmes automatisés qui sont conformes aux valeurs démocratiques et protègent les droits civils, les libertés civiles et la vie privée. **Les cinq principes directeurs sont les suivants : 1) systèmes sûrs et efficaces; 2) protections contre la discrimination algorithmique; 3) confidentialité des données; 4) notifications et explications; et 5) alternatives humaines, considération et recours**. La Déclaration des droits de l'IA comprend un avant-propos, les cinq principes, les notes sur l'application du plan directeur pour une Déclaration des droits de l'IA et les lignes directrices intitulées Des principes à la pratique.

53. Witzel, Mardi, « Quelques questions sur la *Loi sur l'intelligence artificielle et les données* au Canada », IICG, 11 août 2022, en ligne : https://www.cigionline.org/articles/a-few-questions-about-canadas-artificial-intelligence-and-data-act/

Cet article critique la LIAD proposée en soulignant que les questions définissant l'industrie de l'IA (telles que ce qu'est un « système à fort impact » et ce qui constitue un « préjudice important ») sont laissées pour les futures réglementations et que **l'arrangement de gouvernance global dans la LIAD est fondamentalement défectueux** : plus précisément, un seul ministère (ISDE) est responsable à la fois de la rédaction de la loi et de la politique connexe, ainsi que de son administration et de son

application (contrairement au guide de longue date de l'OCDE qui souligne l'importance d'une prise de décision réglementaire indépendante du processus politique).

54. Wylie, Bianca, « Le projet de loi C-27 d'ISDE et la LIAD. Partie 1 : Tech, Human Rights, and the Year 2000 », (9 octobre 2022), en ligne : https://biancawylie.medium.com/iseds-bill-c-27-aida-part-1-tech-human-rights-and-the-year-2000-947088823f4e

L'auteure examine la LIAD et certaines parties du projet de loi C-27 ainsi que les efforts déployés par le gouvernement pour légiférer sur l'IA au Canada. L'article indique que, lorsque le gouvernement a commencé à parler de la nécessité de la LPRPDE à la fin des années 1990, un processus parallèle a été lancé par le Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes (HURAD), qui a fermement exprimé la protection de la vie privée dans le langage des droits de la personne de la Déclaration universelle des droits de l'homme. Le Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes a soutenu que la protection réellement efficace de la vie privée ne peut être maintenue que si l'on accorde plus de poids à la valeur de la vie privée en tant que droit de la personne qu'aux gains d'efficience bureaucratiques et aux avantages économiques d'une circulation sans contrainte de renseignements personnels.

55. Wylie, Bianca, « ISED's Bill C-27 + AIDA. Part 4 : Calling on Federal MPs For a Necessary Defense of Democratic Process », (21 avril 2023), en ligne : https://biancawylie.medium.com/iseds-bill-c-27-aida-part-4-calling-on-federal-mps-for-necessary-defense-of-democratic-process-3003572bc38e (en anglais uniquement)

L'auteure critique l'approche du gouvernement à l'égard de la LIAD qu'elle juge antidémocratique, qualifiant ISDE à la fois de meneur de claque et de marchand de peur pour l'industrie de l'IA. Elle affirme que la LIAD n'a fait l'objet d'aucun débat public large ou à grande échelle et que le grand public, y compris les communautés les plus touchées par les technologies, n'a eu qu'un accès minimal à des discussions éclairées sur l'IA. L'auteure explique que la plupart des organisations et des personnes qui appellent à appuyer la LIAD sont financées par ISDE ou ont des activités professionnelles reposant sur la légitimité de l'IA et que ces personnes ne représentent qu'un ensemble très restreint d'intérêts particuliers qui ne sont pas représentatifs du contexte global du secteur de l'IA. L'auteure examine également la récente réunion d'urgence du Conseil consultatif canadien sur l'IA, convoquée par le ministre d'ISDE, le député Champagne, en soulignant que peu après cette réunion avait été publiée une lettre appelant les membres du Parlement à soutenir la LIAD. L'auteure affirme qu'un tel appel ne représente qu'un concert de voix en circuit fermé et que la lettre signée ne remplace pas la participation officielle et appropriée du grand public à la discussion sur l'IA; elle prévient aussi que ce niveau d'influence des initiés sur l'élaboration des lois est insidieux pour le processus démocratique, empêche une conversation suffisamment large, et effraie et réduit au silence la plupart des membres du public

56. Wylie, Bianca, « We're in an AI hype cycle—can Canada make it a responsible one? », (Centre canadien de politiques alternatives, juillet 2023), en ligne : https://monitormag.ca/articles/were-in-an-ai-hype-cycle-can-canada-make-it-a-responsible-one/

    L'autrice critique le gouvernement fédéral pour son empressement à réglementer l'IA et affirme qu'il devrait se remettre à la table de travail concernant la législation sur l'IA. L'autrice souligne que les exigences de l'éthique administrative publique en la matière devraient faire l'objet d'une discussion, de même que l'adéquation générale dans la rédaction des lois. Elle critique l'approche du gouvernement envers la LIAD, affirmant que si nos élus autorisent ce qui est fait à travers la LIAD, nous serons confrontés à de gros problèmes technologiques et démocratiques. L'autrice estime que, pour gérer les répercussions sociales de l'IA, nous devons bâtir une perspective complètement différente de celle qui a pour objectif principal d'élargir l'industrie canadienne de l'IA. Elle affirme que, même si la LIAD devait faire l'objet d'une révision et d'une correction importantes, nous ne pourrions pas échapper à son objectif principal : normaliser l'utilisation de l'IA dans tous les secteurs de la société.

57. Urban, Jennifer M. & Chris Jay Hoofnagle, « The Privacy Pragmatic as Privacy Vulnerable », (*CUPS, Carnegie Mellon University Security and Privacy Institute*, 2014), en ligne : https://cups. cs. cmu. edu/soupes/2014/ateliers/Privacy/s1p2.pdf >.

    L'article indique que **le modèle de segmentation de la vie privée d'Alan Westin comporte des lacunes structurelles et** qu'il est malheureusement trop cité. Selon Westin, environ la moitié de la population des États-Unis est composée de personnes qui se préoccupent de la protection de la vie privée, qu'on appelle des « **pragmatiques de la protection de la vie privée** ». Cette conclusion a été utilisée pour promouvoir un régime de protection de la vie privée fondé sur le choix qui, comme par hasard, est favorable aux grandes sociétés qui ont appuyé la recherche de Westin. L'article conclut que le modèle de segmentation de la protection de la vie privée **devrait être utilisé avec parcimonie, voire pas du tout**.

58. Young, David, « Non-Identifiable Information Under Bill C-27 », (30 septembre 2022), en ligne : http://davidyounglaw.ca/compliance-bulletins/non-identifiable-information-under-bill-c-27/

    L'auteur examine le cadre du projet de loi C-27 pour les renseignements non identifiables et constate qu'il s'aligne sur des cadres analogues du RGPD de l'Union européenne, de la loi québécoise modifiée et des propositions envisagées pour une loi ontarienne sur la protection de la vie privée et une loi réformée en Colombie-Britannique. L'auteur signale plusieurs points à améliorer dans le projet de loi et affirme qu'**à l'avenir, un aspect important des lois sur la protection de la vie privée fournira un cadre justifiable pour les renseignements non identifiables et l'IA éthique**.

59. Young, David, « OPC appeals Federal Court's Facebook decision not requiring it to change its privacy practices », (davidyounglaw.com), en ligne : https://davidyounglaw.ca/compliance-bulletins/opc-appeals-federal-courts-facebook-decision-not-requiring-it-to-change-its-privacy-practices/

L'auteur traite de l'appel interjeté par le CPVP à l'égard de la décision de la Cour fédérale de ne pas exiger que Meta (anciennement Facebook) modifie ses politiques et procédures en matière de protection de la vie privée, ayant mené à l'atteinte à la protection des données par Cambridge Analytica. L'auteur examine la décision de la Cour fédérale sur laquelle l'appel est fondé, affirmant qu'elle contient des décisions problématiques concernant la LPRPDE, ainsi que la nature de la preuve requise dans le cadre d'une demande en justice visant à faire respecter les conclusions du CPVP. L'article précise que le troisième principe de la LPRPDE a été interprété à tort comme une réserve fondamentale à l'obligation d'obtenir un consentement valable, et conclut notamment qu'il faut plus qu'un « effort raisonnable » pour établir l'obtention d'un consentement valable. L'auteur souligne également la conclusion de la Cour selon laquelle une simple lecture des politiques de Facebook ne suffisait pas à conclure que Meta n'avait pas fait un effort raisonnable d'information des utilisateurs de l'utilisation potentielle de leurs données. L'article compare la norme de la « personne raisonnable » établie par la Cour au critère prévu par la *Loi sur la concurrence*, qui utilise un critère objectif pouvant s'appliquer à un éventail de situations de fait et à différents niveaux de complexité ou de crédulité.

Liens avec la législation pertinente

Canada – Fédéral

60. Le projet de loi C-27, la Loi édictant la « *Loi sur la protection de la vie privée des consommateurs* », la *Loi sur le Tribunal de la protection des renseignements personnels et* des *données* et la *Loi sur l'intelligence artificielle et les données* et apportant des modifications connexes et corrélatives à certaines lois, première session, quarante-quatrième législature, juin 2022, en ligne : https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

61. La Loi canadienne antipourriel (LCAP), la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications,* L.C. 2010, c. 23, en ligne : https://laws-lois.justice.gc.ca/fra/lois/e-1.6/index.html.

62. *Loi électorale du Canada*, L.C. 2000, c. 9, en ligne : https://laws.justice.gc.ca/fra/lois/e-2.01/index.html.

63. *Loi sur la concurrence*, L.R.C. 1985, c. C-34, en ligne : https://laws.justice.gc.ca/fra/lois/c-34/index.html

64. Ancien projet de loi C-11, *Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois,* 44e législature, deuxième session, novembre 2020, en ligne : https://www.parl.ca/DocumentViewer/fr/43-2/projet-loi/C-11/premiere-lecture

65. *Loi sur la protection des renseignements personnels et les documents électroniques,* S.C. 2000, c. 5 https://laws.justice.gc.ca/fra/lois/P-8.6/index.html

Canada – Provinces

66. La loi de l'Alberta *Personal Information Protection Act*, chapitre P-6.5, en ligne : https://kings-

printer.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779831562&display=html

67. La loi britanno-colombienne *Personal Information Protection Act*, SBC 2003, chapitre 63, en ligne : https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01

68. La *Loi 25* du Québec (ancien Projet de loi 64), la *Loi visant à moderniser des dispositions législatives en matière de protection des renseignements personnels,* étant

> *la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1)* en ligne :
>
> https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1
>
> lu conjointement avec le projet de loi n° 64, *Loi visant à moderniser des dispositions législatives concernant la protection des renseignements personnels* (les dispositions pertinentes étant les articles 93 à 152) en ligne :
>
> http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C25A.PDF

> Version administrative française en ligne de la *Loi sur la protection des renseignements personnels dans le secteur privé* (*Act respecting the protection of personal information in the private sector*) préparée par la Commission d'accès à l'information du Québec; et

> Version administrative anglaise en ligne de la *Loi sur la protection des renseignements personnels dans le secteur privé* préparée par le cabinet d'avocats canadien BLG.

Union européenne

69. *Union* européenne, *Règlement sur la gouvernance des données*, 2022, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R0868

70. *Règlement général de l'Union européenne sur la protection des données*, Règlement (UE) 2016/679, en ligne : https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679

71. *Proposition* de l'Union européenne pour une *Loi sur l'intelligence artificielle,* en ligne : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

72. *Union* européenne, *Directive sur la protection des lanceurs d'alerte*, Directive (UE) 2019/1937, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019L1937

Royaume-Uni

73. Royaume-Uni, *Data Protection Act*, 2018, en ligne : https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

74. La *loi* de la Colombie-Britannique *Personal Information Protection Act*, SBC 2003, chapitre 63, en ligne : https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01

75. Royaume-Uni, *Data Protection and Digital Information (no. 2) Bill*, en ligne : https://commonslibrary.parliament.uk/research-briefings/cbp-9803/

États-Unis

76. États-Unis, *American Data Privacy and Protection Act*, en ligne : https://www.congress.gov/bill/117th-congress/house-bill/8152/text

77. États-Unis, *Data Elimination and Limiting Extensive Tracking and Exchange Act* (la « **Loi DELETE** ») en ligne : https://www.congress.gov/bill/117th-congress/senate-bill/3627/text

78. Californie, *The California Age-Appropriate Design Code Act*, 2022 en ligne : https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

79. California, *The California Privacy Act of 2018*, en ligne : https://oag.ca.gov/privacy/ccpa

80. Californie, *The California Privacy Act Regulations*, en ligne https://oag.ca.gov/privacy/ccpa

81. Californie, *Delete Act*, en ligne : https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362

82. Colorado, *Privacy Act*, 2021, en ligne : https://coag.gov/resources/colorado-privacy-act/ https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

83. Connecticut, *Data Privacy Act*, 2022, en ligne : https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

84. Utah, *Consumer Privacy Act*, 2022, en ligne : https://le.utah.gov/~2022/bills/static/SB0227.html

85. Virginie, *Consumer Data Protection Act*, 2021, en ligne : https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

Nations Unies

86. *Déclaration des Nations Unies sur les droits des peuples autochtones* (DNUDPA), Rés. AG 61/295, en ligne : https://social.desa.un.org/sites/default/files/migrated/19/2018/11/UNDRIP_F_web.pdf