SEPTEMBRE 2021

Commentaires du CIPVP sur le livre blanc du gouvernement de l'Ontario intitulé *Modernisation de la protection de la vie privée en Ontario*

Patricia Kosseim
Commissaire

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Table des matières

A. INTRODUCTION

Le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) se réjouit de pouvoir commenter le livre blanc du gouvernement intitulé *Modernisation de la protection de la vie privée en Ontario.*[1] Par nos commentaires et recommandations, nous souhaitons appuyer la création d'un cadre réglementaire moderne fondé sur une rigoureuse gouvernance des renseignements personnels dans le secteur privé, qui ne laisse aucun Ontarien pour compte. Un tel cadre devrait permettre une innovation responsable et viable, faciliter une surveillance transparente entre les secteurs et assurer l'harmonisation avec les autres territoires de compétence.

Je félicite le gouvernement de proposer des dispositions concrètes conformes à l'approche fondée sur des principes, équitable, équilibrée, pragmatique, souple et proportionnée qu'a demandées notre bureau dans sa réponse[2] au premier document de discussion intitulé *Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique* que le gouvernement a publié en août dernier.[3] Nous sommes d'avis que l'Ontario devrait saisir cette occasion pour atteindre l'objectif de la province de permettre aux Ontariens d'acquérir « *les compétences, les droits et les possibilités nécessaires pour participer pleinement au monde numérique, y travailler et s'y épanouir* »[4] et de protéger leurs renseignements personnels d'une manière conforme aux valeurs, aux réalités et à la culture du milieu. Le livre blanc est une étape essentielle dans la mise en place d'un paysage moderne de protection de la vie privée en Ontario, qui donnera au public la confiance dont il a besoin pour adopter l'innovation plutôt que de s'en méfier. Il importe également de fournir une assurance réglementaire et un soutien en matière de conformité aux entreprises ontariennes, en particulier aux petites et moyennes entreprises (PME), pour promouvoir l'économie axée sur les données à un moment où les Ontariens en ont le plus besoin.

L'harmonisation était manifestement un facteur important dans la décision du gouvernement de fonder ses propositions législatives sur la *Loi de 2020 sur mise en œuvre de la Charte du numérique* (le projet de loi C-11), en l'élargissant et en l'améliorant au besoin et selon ce qui convient aux Ontariens. Nous jugeons cette approche judicieuse étant donné l'importance d'obtenir le statut « essentiellement similaire », qui exempterait les organisations ontariennes menant des activités commerciales dans la province du régime fédéral[5], simplifierait la surveillance réglementaire et assurerait la compatibilité pratique avec d'autres régimes de protection de la vie privée dans le secteur privé au Canada et dans le monde.

Avant de commenter chacun des sept « domaines clés de la réforme » que propose le livre blanc, nous estimons nécessaire de répondre à la déclaration du ministre[6] qui accompagne le livre blanc et qui laisse entendre que la réforme du secteur privé en Ontario dépendrait du sort du projet de loi C-11. Depuis cette déclaration, nous avons appris que le projet de loi C-11 allait mourir au feuilleton avec la récente annonce d'une élection fédérale à l'automne. Le prochain gouvernement fédéral pourrait déposer la même version du projet de loi, une version modifiée ou un tout nouveau projet de loi ou tout annuler. Devant une

telle incertitude, le gouvernement de l'Ontario doit poursuivre ses démarches visant à améliorer le droit à la protection de la vie privée pour les Ontariens.

B. LA NÉCESSITÉ D'UNE ACTION PROVINCIALE, AVEC OU SANS RÉFORME FÉDÉRALE

Comme indiqué précédemment, le bureau du commissaire estime que le droit à la protection de la vie privée serait mieux protégé par une loi provinciale sur la protection de la vie privée qui serait essentiellement similaire à la loi fédérale, mais qui irait au-delà des limites de l'actuelle *Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE*), du projet de loi C-11 ou de tout autre projet de réforme qui pourrait être présenté à l'avenir.

Trois provinces canadiennes ont déjà adopté des lois sur la protection de la vie privée dans le secteur privé qui s'apparentent à la *LPRPDE*. L'Ontario, la plus grande province du Canada, doit décider de faire partie des provinces (ou en être le chef de file) qui ont choisi de protéger leurs citoyens en comblant les lacunes réglementaires qu'a créées le cadre fédéral.

Sans une approche provinciale de la protection de la vie privée en Ontario, des millions d'Ontariens s'exposeront encore aux risques associés à l'absence de réglementation en matière de protection de la vie privée et de la sécurité, ce qui pourrait ébranler la confiance du public dans l'économie ontarienne axée sur les données.

Dans la discussion qui suit, nous expliquons en quoi les Ontariens et les entreprises en exploitation dans cette province profiteraient d'une loi sur la protection de la vie privée dans le secteur privé soigneusement élaborée en Ontario, que la réforme de la loi fédérale ait lieu ou non.

1) LIMITES DE COMPÉTENCE

Qui plus est, une loi provinciale sur la protection de la vie privée dans le secteur privé pourrait fournir des protections dans des domaines où le parlement fédéral n'a pas compétence pour agir. Plus précisément, le CIPVP a été encouragé par la proposition du gouvernement d'inclure les employés des entreprises sous réglementation provinciale qui ne bénéficient d'aucune protection en vertu de la loi fédérale sur la protection de la vie privée.[7] De même, nous avons été heureux de constater que la loi provinciale envisagée protégerait les syndicats, les organismes de bienfaisance et les associations professionnelles dont les activités non commerciales sont sans réglementation depuis trop longtemps. Une loi ontarienne sur la protection de la vie privée dans le secteur privé pourrait offrir des protections complètes entièrement hors de portée de toute loi fédérale actuelle ou future.

I. EMPLOYÉS

Les droits à la protection de la vie privée des employés d'entreprises sous réglementation provinciale ne sont pas et ne seront jamais protégés par une loi fédérale sur la protection de la vie privée, compte tenu des contraintes d'ordre constitutionnel. Bien des experts ont exprimé des inquiétudes sur le degré croissant de surveillance des employés pendant la pandémie de COVID-19[8], ce qui pourrait ne pas s'atténuer après coup. La professeure Teresa Scassa a décrit certaines nouvelles technologies permettant aux employeurs de suivre la productivité de leurs employés. Celles-ci incluent les technologies qui surveillent les sites Web consultés, le temps passé sur des sites Web ou dans des documents, des renseignements de localisation par GPS, les écrans d'ordinateur des employés, les courriels entrants et sortants, les frappes au clavier, l'activité sur les médias sociaux, etc. Des technologies encore plus envahissantes, dont celles de reconnaissance faciale et d'analyse des sentiments exprimés par la voix, pourraient bientôt se profiler à l'horizon. De nombreux employeurs[9] envisagent d'exiger que leurs employés fournissent une preuve vaccinale comme condition de travail, soit d'autres risques d'atteinte à la vie privée et à d'autres droits de la personne qui devront être justifiés, gérés et atténués sur le plan juridique en fonction du contexte et des circonstances propres à l'emploi.

Étant donné le manque actuel de protection au quotidien pour des millions d'Ontariens qui s'efforcent de gagner leur vie, le fait de combler les lacunes en matière de protection de la vie privée des employés serait un accomplissement majeur.

II. SECTEUR SANS BUT LUCRATIF

Les grands volumes de données que détient le secteur sans but lucratif en Ontario ne sont pas à l'abri des vulnérabilités en matière de protection de la vie privée et de sécurité,[10] néanmoins, ils restent largement non protégés par les dispositions fédérales sur la protection de la vie privée, dont la portée est limitée par la Constitution. La pandémie n'a fait qu'exacerber les cybermenaces qui pèsent sur le secteur non commercial. Comme bien d'autres secteurs, les organisations sans but lucratif ont de plus en plus recours au télétravail, ce qui accroît l'exposition aux risques pour la vie privée et la sécurité.[11] Outre ces risques, les organismes sans but lucratif peuvent avoir moins de ressources à consacrer aux activités de conformité en matière de protection de la vie privée. Par exemple, un organisme offrant des services de repas ayant récemment été victime d'une violation de la vie privée a mis cinq mois à informer (volontairement) les particuliers touchés, car la modeste équipe de l'organisme a dû déployer beaucoup de temps et d'effort pour évaluer la violation et intervenir en conséquence.[12] Aucune loi sur la protection de la vie privée ne s'applique de manière générale aux organismes sans but lucratif de l'Ontario, et la responsabilité à l'égard de ce secteur n'incombe à aucun organisme de réglementation. En vertu d'une loi provinciale sur la protection de la vie privée dans le secteur privé, le CIPVP aurait le mandat élargi de soutenir les organismes sans but lucratif en les conseillant sur leurs défis en matière de protection de la vie privée et de sécurité, en les informant des risques et en encourageant les protections en amont.

III. PARTIS POLITIQUES

Bien que les propositions du gouvernement n'abordent pas ce sujet, le CIPVP recommande qu'une loi ontarienne sur la protection de la vie privée dans le secteur privé s'applique aux partis politiques, comme c'est le fait la loi sur la protection de la vie privée dans le secteur privé de la Colombie-Britannique[13] et comme le propose le projet de loi 64 du Québec.[14] L'importance d'inclure les partis politiques dans le champ d'application d'une loi sur la protection de la vie privée a beaucoup été soulevée, y compris par l'agent indépendant de l'Ontario responsable de la surveillance des élections qui a demandé que les dispositions législatives les régissent.[15] Les récentes actualités ayant mis au jour l'utilisation présumée de la technologie de reconnaissance faciale par les partis politiques pour vérifier les identités[16] ou le scandale de Cambridge Analytica suffisent pour comprendre la nécessité d'imposer aux partis politiques des obligations de protection de la vie privée. L'éventuelle utilisation abusive des renseignements personnels dans les campagnes électorales risque d'ébranler non seulement la confiance des citoyens, mais aussi la démocratie.

2) JEUNES ET ENFANTS

S'il est généralement compris que les enfants et les jeunes méritent une protection spéciale de la vie privée vu leur vulnérabilité inhérente, la *LPRPDE* et le projet de loi C-11 abordent à peine ce sujet. La province a l'occasion de combler cette lacune en adoptant une loi, accompagnée de règlements ou de codes de pratique, qui protège ses citoyens les plus vulnérables.

Vingt et un pour cent des élèves ontariens interrogés (de la 7e à la 12e année) en 2019 ont indiqué passer cinq heures ou plus sur les médias sociaux par jour.[17] Des études réalisées depuis le début de la pandémie de COVID-19 ont montré une augmentation significative du temps passé devant l'écran et de l'utilisation des médias sociaux, tant chez les enfants que chez les jeunes.[18] L'augmentation du temps passé en ligne accroît le risque que les renseignements personnels des enfants soient utilisés à mauvais escient, voire usurpés d'une manière qui peut leur être préjudiciable, ce qui porte gravement atteinte à leur sentiment d'identité, à leur confiance en soi et à leur bien-être. Comme nous l'avons indiqué dans notre précédent document, les jeunes devraient avoir la liberté d'expérimenter et de se découvrir dès le plus jeune âge sans avoir à se soucier des répercussions permanentes sur leur réputation des renseignements qu'ils publient en ligne.

Les risques pour la vie privée des enfants et des jeunes ne se limitent pas aux médias sociaux. Les nouveaux jouets intelligents intègrent des capacités d'intelligence artificielle (IA) qui permettent de recueillir des données afin de personnaliser l'expérience utilisateur des enfants.[19] L'utilisation de ces jouets intelligents va s'accroître, et les enfants méritent d'être protégés contre les technologies potentiellement intrusives, plus précisément celles qui sont conçues pour les sonder, créer une accoutumance aux jeux, ou influencer négativement leur comportement de toute autre manière.

Étant donné le lien provincial avec l'éducation, une loi provinciale sur la protection de la vie privée dans le secteur privé pourrait contribuer à améliorer la protection de la vie privée des enfants dans les écoles. Bien que le CIPVP ait compétence à l'égard des commissions scolaires en vertu de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP), nous n'avons pas de compétence directe sur les entreprises tierces avec lesquelles elles passent des marchés de services de traitement de l'information, tels que des services de gestion des données en nuage ou l'utilisation de plateformes numériques à des fins scolaires. Comme l'indiquent deux récents constats de notre bureau, cela signifie que si les choses tournent mal avec un fournisseur de services tiers, nous ne pouvons enquêter que sur une partie du problème.[20]

3) EFFICIENCES OPÉRATIONNELLES

En l'absence d'une loi substantiellement similaire en Ontario, la *LPRPDE* s'applique à l'ensemble des entreprises canadiennes — des géants mondiaux de l'Internet, des grandes multinationales, des banques et des entreprises de télécommunications aux petites entreprises émergentes et aux entreprises familiales — dont les réalités et les niveaux de risque diffèrent. Il en serait de même dans le cas du projet de loi C-11 ou de tout autre projet de réforme fédérale.

Dans le secteur économique de l'Ontario, les PME composent 98 % de toutes les entreprises de la province et 30 % du PIB de la province.[21] La proposition de l'Ontario tend vers une approche plus souple et mieux adaptée aux réalités des PME et aux défis en matière de conformité qui leur sont propres. Selon la proposition de l'Ontario, le CIPVP serait investi du pouvoir discrétionnaire de créer des outils de soutien à la conformité, tels que des services consultatifs, et d'approuver la création de codes de pratique sectoriels et de programmes de certification. En raison de la géographie de la province, le CIPVP pourrait jouer un rôle consultatif à l'échelle régionale et locale, plus sensible aux réalités du secteur des PME. En adaptant le matériel éducatif, les codes et les services consultatifs pour mieux tenir compte de la situation sur le terrain et en disposant d'un certain pouvoir discrétionnaire pour s'attarder aux aspects étant les plus concrets, le CIPVP pourrait aider les PME dans leurs efforts pour se relever de la pandémie de COVID-19 et pour adopter des solutions plus permanentes. Le CIPVP pourrait par ailleurs aider les petites entreprises en démarrage innovantes à prospérer et à croître de manière responsable, en accord avec la Stratégie ontarienne pour le numérique et les données.[22]

La proposition de l'Ontario garantirait un régime de conformité équitable, contextuel et robuste, plus rationnel et plus efficace. L'Ontario pourrait concevoir un mécanisme souple et proportionné de règlement des différends qui serait moins fastidieux que le régime de conformité à deux niveaux que propose le projet de loi C-11. Les Ontariens ont plus de 30 ans d'expérience du mécanisme de règlement des différends en matière d'accès à l'information et de protection de la vie privée du CIPVP, qui est fortement fondé sur la résolution précoce et la médiation.[23] Les tribunaux de l'Ontario connaissent bien les

processus d'adjudication du CIPVP, car ils ont établi une importante jurisprudence sur les questions d'examen judiciaire dont ils ont été saisis au cours des dernières décennies.

4) INTÉGRATION INTERSECTORIELLE

La proposition de l'Ontario permet de créer un environnement réglementaire transparent en matière de données, mieux intégré entre les secteurs, ce qu'une loi fédérale ne pourrait accomplir concrètement. Le gouvernement de l'Ontario peut réduire les formalités administratives et le fardeau réglementaire en ayant une approche réglementaire en accord avec des initiatives intersectorielles innovantes et la croissance exponentielle des partenariats publics-privés (PPP), du secteur des technologies éducatives aux services de soins de santé virtuels, en passant par les villes intelligentes. Le recours à des fournisseurs de services tiers étant de plus en plus courant et le nombre croissant d'atteintes aux données survenant quelque part dans la chaîne de traitement des renseignements, l'Ontario pourrait réglementer les différents éléments de l'ensemble au sein d'un seul territoire de compétence, plutôt que de jongler avec plusieurs lois provinciales (pour les composantes du secteur public, de la santé, de l'enfance et de la jeunesse) et la loi fédérale (pour les composantes du secteur privé).

Une loi ontarienne sur la protection de la vie privée dans le secteur privé relevant d'une même compétence pourrait être soigneusement élaborée de manière à ce que ses dispositions s'inspirent d'autres lois sur la protection des renseignements personnels et l'accès à l'information dans les secteurs de la santé, de l'enfance et de la jeunesse, et dans le secteur public ou aient préséance sur celles-ci. L'Ontario pourrait donc adopter une approche cohérente en intégrant une nouvelle loi sur la protection de la vie privée dans le secteur privé et ses autres lois sur la protection des renseignements personnels et l'accès à l'information, toutes régies par un seul organisme de réglementation de la protection de la vie privée, dont le mandat serait soigneusement agencé avec la nouvelle autorité en matière de données proposée dans le cadre de sa stratégie numérique et de données.[24] L'Ontario pourrait donc simplifier les exigences de conformité, accroître la certitude réglementaire pour les organisations de PPP participantes et rationaliser l'environnement réglementaire des données de l'Ontario en général.

5) APPROCHE HARMONISÉE

Un autre facteur à prendre en compte pour une loi ontarienne sur la protection de la vie privée consiste à savoir réglementer l'activité commerciale dont les flux de données transfrontaliers font partie intégrante de l'économie mondiale. Quant aux craintes qu'une loi ontarienne sur la protection de la vie privée dans le secteur privé ne complexifie le paysage législatif canadien, un régime moderne de protection de la vie privée pourrait intégrer les mécanismes nécessaires pour réduire le fardeau réglementaire imposé aux entreprises qui doivent se conformer à des lois relevant de plusieurs territoires de compétence. Ce défi existe déjà pour d'innombrables autres activités réglementées en

vertu du statut de fédération du Canada et peut être surmonté par des choix de conception intentionnels, créatifs et stratégiques qui favorisent le fédéralisme coopératif.

Par exemple, la *LPRPDE* reconnaît explicitement le pouvoir législatif des provinces de réglementer la collecte, l'utilisation et la communication des renseignements personnels sur leur territoire respectif. Si une province choisit d'adopter une loi provinciale « essentiellement similaire » — comme l'ont déjà fait le Québec, la Colombie-Britannique et l'Alberta —, les entreprises qui exercent des activités commerciales dans cette province sont exemptées de la *LPRPDE* et doivent uniquement se conformer à la loi provinciale en question. Pour les entreprises qui exercent une activité commerciale transfrontalière et qui peuvent être soumises à la loi fédérale sur la protection de la vie privée, le concept de « essentiellement similaire » aide à assurer l'harmonisation et l'interopérabilité entre les territoires de compétence canadiens.[25] Dans la même veine, pour ce qui est de la circulation internationale des données, le concept du « statut d'adéquation » encourage l'harmonisation et l'interopérabilité avec le *Règlement général sur la protection des données* (RGPD) de l'Union européenne.[26]

De plus, les accords existants entre les autorités canadiennes chargées de la protection de données permettent déjà des mesures d'application coopératives qui offrent une meilleure protection à leurs résidents, une prévisibilité et une certitude accrues pour les entreprises, et une réduction du fardeau réglementaire. La loi ontarienne dans le secteur privé pourrait permettre ou autoriser explicitement la conclusion de régimes d'échange de renseignements entre le CIPVP et d'autres commissaires à la protection de la vie privée fédéraux, provinciaux et territoriaux (FPT), ainsi que d'autres organismes de réglementation pertinents, afin de promouvoir l'uniformité des approches et la conformité coopérative. En vertu de tels régimes, les organismes de réglementation pourraient se respecter les uns les autres, s'engager à respecter des principes fondamentaux communs, s'entendre sur des indicateurs aidant à déterminer le territoire de compétence principal et se consulter pour relever les lacunes à combler et les domaines de collaboration continue.

Enfin, en matière de conformité, les pouvoirs d'ordonnance du CIPVP, y compris le pouvoir d'imposer des sanctions administratives en vertu d'une loi ontarienne sur la protection de la vie privée dans le secteur privé, pourraient prendre en compte de toute mesure réglementaire déjà prise par d'autres territoires de compétence comme facteur atténuant possible, assurant une approche harmonisée, équitable et proportionnée.

Pour les raisons susmentionnées, le CIPVP encourage le gouvernement à présenter sa propre loi sur la protection de la vie privée dans le secteur privé, sans égard à la réforme de la loi fédérale en la matière. Cette occasion législative mérite d'être poursuivie au profit de tous les Ontariens, et pas seulement comme un plan de repli pour le projet de loi C-11 ou tout autre projet de loi qui lui succéderait et dont l'avenir est plus qu'incertain.

C. COMMENTAIRES SUR LES DOMAINES DE RÉFORME QUE PROPOSE LE GOUVERNEMENT

Nous passons maintenant à chacun des sept sujets que le gouvernement a soulevés dans son livre blanc sous la rubrique « Domaines clés de la réforme ». Nous espérons que notre point de vue aidera les délibérations du gouvernement et stimulera le débat public constructif que le livre blanc est censé susciter.

1. APPROCHE FONDÉE SUR LES DROITS

I. PRÉAMBULE

Le CIPVP applaudit la proposition du gouvernement d'affirmer que la vie privée est un droit fondamental dans le préambule d'une éventuelle loi ontarienne sur la protection de la vie privée. Selon la professeure Teresa Scassa, titulaire de la chaire de recherche du Canada en politiques et droit de l'information à l'Université d'Ottawa, l'inclusion de considérants dans un préambule énonçant les fondements de la protection de la vie privée en matière de droits de la personne donnerait une voix législative aux principes et aux valeurs des droits de la personne qui sous-tendent la loi sur la protection des données au Canada et fournirait un cadre concret pour l'interprétation de ses dispositions.[27] Bien que la LPRPDE ait été jugée comme ayant un statut quasi constitutionnel,[28] une décision récente[29] de la cour fédérale renforce le besoin de rendre l'approche des droits de la personne plus explicite si elle doit « transformer ou modifier l'approche appropriée de l'interprétation des lois ».[30]

Dans son livre blanc, le gouvernement de l'Ontario a indiqué qu'« un facteur clé pour établir la confiance du public dans le droit à la vie privée sera la mise en place de véritables exigences de transparence et d'une surveillance forte et indépendante pour les Ontariens ». Pourtant, aucun de ces principes n'est évoqué dans le préambule proposé. Pas plus que le concept de responsabilité démontrable. La transparence et la responsabilité sont sans doute deux des principes les plus fondamentaux d'une loi moderne sur la protection de la vie privée, qui méritent au moins la même importance que les principes de proportionnalité, d'équité et d'adéquation. En fait, la plupart des lois modernes sur la protection de la vie privée voient l'« indépendance » des autorités de protection des données comme un élément essentiel pour une surveillance efficace.[31] Une référence explicite à la surveillance indépendante s'accorderait sur les objectifs primordiaux énoncés dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) de l'Ontario.

II. DES OBJECTIFS JUSTES ET APPROPRIÉS

Le gouvernement de l'Ontario a proposé une disposition générale qui fixerait des « limites fondées sur des principes » au sujet des activités autorisées par la loi. Cette

disposition garantirait que les renseignements personnels ne peuvent être recueillis, utilisés ou divulgués qu'à des fins qu'une personne raisonnable considérerait comme justes et appropriées dans les circonstances. Nous applaudissons l'application proposée de la clause juste et appropriée à toutes les collectes, utilisations ou divulgations de renseignements personnels, avec ou sans consentement. Cette disposition contribuera à transformer ce qui pourrait être interprété comme un simple symbole de conformité par des traces écrites documentant la conformité technique[32] en une protection plus substantielle du droit à la vie privée des Ontariens.

Le principe d'équité n'est pas inclus dans la disposition sur les fins appropriées de la *LPRDE* ou du projet de loi C-11, et nous félicitons le gouvernement d'envisager l'introduction de ce concept important comme condition primordiale. Le Comité européen de la protection des données (CEPD) définit la loyauté comme « un principe général qui exige que les données à caractère personnel ne soient pas traitées d'une manière qui soit préjudiciable, discriminatoire, inattendue ou trompeuse pour la personne concernée. »[33] Ce concept est d'une importance capitale pour protéger les particuliers et les groupes des facteurs discriminatoires en aval du traitement et du profilage automatisés des données, par exemple.

Nous applaudissons également le gouvernement, qui a codifié une liste de facteurs objectifs devant être pris en compte lors de l'évaluation de ce qu'une personne raisonnable considérerait comme un objectif juste et approprié. Ces facteurs offrent une plus grande prévisibilité et une plus grande certitude aux organisations qui doivent appliquer la loi et aux régulateurs et tribunaux qui doivent l'interpréter.

En ce qui concerne les facteurs proposés eux-mêmes, nous formulons trois commentaires. Tout d'abord, lorsque l'on considère le volume, la nature et la sensibilité des renseignements personnels, nous recommandons d'inclure la prise en compte du contexte. Pour des raisons que nous développons ci-dessous, la sensibilité de l'information peut changer radicalement d'un contexte à l'autre.

Deuxièmement, en évaluant si les renseignements personnels sont nécessaires pour répondre aux besoins légitimes de l'organisation, il faut également tenir compte de l'efficacité. Si la collecte, l'utilisation ou la divulgation des renseignements personnels n'est pas susceptible d'être efficace pour répondre aux besoins légitimes d'une organisation, elle n'est pas non plus susceptible d'être nécessaire pour atteindre les mêmes fins insaisissables. Inversement, même si la collecte, l'utilisation ou la communication de renseignements personnels est efficace pour répondre aux besoins légitimes d'une organisation, il pourrait ne pas être nécessaire de le faire lorsque, par exemple, moins de renseignements personnels ou d'autres renseignements personnels suffisent. Pour plus de certitude, nous recommandons que le facteur proposé fasse explicitement référence à la fois à la nécessité et à l'efficacité comme conditions d'accompagnement à prendre en compte pour déterminer ce qui est juste et approprié[34].

Troisièmement, au moment d'évaluer si l'avantage est proportionnel à la perte de vie privée de la personne, il serait important de préciser à qui profite l'avantage. Nous recommandons que l'avantage soit considéré au-delà du pur profit commercial de l'organisation pour inclure les avantages pour le particulier, pour d'autres personnes, et pour la société, au sens plus large.

III. « ZONES INTERDITES »

Les « besoins légitimes » d'une organisation figurent parmi la liste des facteurs qui doivent être pris en compte pour évaluer ce qui constitue un objectif juste et approprié.[35] Le livre blanc propose un sous-paragraphe de l'énoncé d'objectifs équitables et appropriés dans lequel il énumère ce qui ne serait *pas* considéré comme un besoin légitime d'une organisation. Si l'intention du gouvernement est d'interdire complètement ces pratiques désignées (nous sommes fermement convaincus qu'il devrait le faire), nous recommandons qu'il le fasse de manière plus claire, directe et explicite en déclarant qu'il ne s'agit *pas* d'objectifs équitables et appropriés, plutôt que de façon indirecte en ne devant les prendre en compte que lors de l'évaluation des besoins légitimes.

Parmi la liste des objectifs interdits (également appelés « zones interdites ») figurent les objectifs dont on sait qu'ils causent ou sont susceptibles de causer un préjudice important à des particuliers ou à des groupes; les contraventions à une loi de l'Ontario ou du Canada; la surveillance ou le profilage d'une personne âgée de moins de 16 ans dans le but d'influencer son comportement ou ses décisions; et toute autre fin prescrite. Avec une réserve, nous soutenons l'inclusion de ces zones interdites dans la loi.

Nous nous demandons notamment si l'interdiction de surveiller ou de profiler les enfants et les jeunes dans le but d'influencer leur comportement ou leurs décisions ne serait pas formulée de manière trop large. Étant donné qu'une loi ontarienne s'appliquerait notamment aux organismes à but non lucratif, cette interdiction pourrait, par inadvertance, empêcher des initiatives éducatives qui profitent réellement aux enfants et aux jeunes en favorisant des changements de comportement positifs (p. ex., l'adoption de choix alimentaires plus sains ou la pratique d'une activité physique accrue), plus précisément dans les cas où le consentement des parents a été obtenu à cette fin. En conséquence, nous recommandons au gouvernement d'envisager de qualifier cette zone d'interdiction aux cas qui peuvent « *influencer négativement* le comportement ou les décisions du particulier ».

IV. DÉFINITIONS DES TERMES « RENSEIGNEMENTS PERSONNELS » ET « RENSEIGNEMENTS SENSIBLES »

Le livre blanc a sollicité des commentaires sur la définition des renseignements personnels. Il existe un ensemble de lois et de jurisprudence de longue date qui définissent les renseignements personnels comme « les renseignements concernant un particulier

identifiable ». Étant donné l'importance d'une approche harmonisée, nous recommandons qu'une nouvelle loi ontarienne soit conforme à cette définition déjà bien établie dans de nombreuses lois sur la protection de la vie privée en Ontario, au Canada et à l'étranger[36].

Toutefois, trois aspects de cette définition méritent plus d'attention. Premièrement, le concept d'identifiabilité est devenu de plus en plus fluide, notamment lorsqu'on tient compte des risques de réidentification. Nous développons ce point plus loin dans notre discussion sur la dépersonnalisation.

Deuxièmement, la question de savoir si des renseignements sont « au sujet » d'un particulier a été mise à rude épreuve, car les nouvelles technologies peuvent déduire ou prédire des renseignements sur un particulier sur la base d'analyses de son comportement ou de son profil en ligne. Que ces renseignements soient exacts ou ne le soient pas ne devrait pas peser dans la balance pour ce qui est de la protection de la vie privée. S'ils sont associés à un particulier ou lui sont attribués par un humain ou un algorithme, il faut les traiter comme étant *au sujet* de ce particulier.

Troisièmement, il y a le concept du particulier. Bien que les lois sur la protection de la vie privée aient été toujours centrées sur le particulier, on reconnaît de plus en plus les violations potentielles de la vie privée (et les effets discriminatoires en aval) que les nouvelles technologies de l'information, notamment l'IA, peuvent avoir sur des groupes. S'il est peut-être trop tôt pour proposer une modification de la définition classique des renseignements personnels sans réfléchir davantage aux ramifications potentielles, les répercussions sur les groupes devraient être prises en compte dans d'autres dispositions d'une loi moderne sur la protection de la vie privée, chaque fois que cela est pertinent et approprié.

Le livre blanc invite également à donner son avis sur la question de savoir si les renseignements sensibles doivent être définis dans la loi en fonction du risque ou de classes ou catégories d'information en particulier. Nous ne recommandons pas de définir la sensibilité sous la forme d'une liste énumérée de types de données. À maintes reprises, des affaires ont montré que des renseignements qui peuvent sembler banals à première vue (p. ex., des renseignements sur les abonnés) peuvent atteindre le niveau de « sensibilité » en fonction de ce que ces renseignements ajoutés à d'autres renseignements peuvent révéler sur le particulier dans les circonstances[37]. Inversement, les renseignements présumés sensibles par nature (p. ex., les renseignements financiers) peuvent être considérés comme moins sensibles en fonction du contexte particulier[38]. À notre avis, la sensibilité des renseignements est certainement un facteur approprié à prendre en compte pour déterminer ce qui constitue une fin équitable et appropriée, si le consentement doit être exprès ou implicite, le niveau de mécanisme de sécurité qui est justifié et si une violation des données pose un risque réel de préjudice grave, etc. La protection plus élevée accordée aux renseignements sensibles peut également être pertinente pour évaluer le caractère adéquat d'une loi ontarienne sur la protection de la vie privée dans le secteur privé en vertu du Règlement général sur la protection des données[39]. Cependant, dans l'évaluation de la sensibilité, la nature de l'information ne doit jamais, selon nous, être dissociée de son contexte.

V. PORTABILITÉ DES DONNÉES

La proposition du gouvernement en matière de portabilité des données accorderait aux particuliers le droit de transférer leurs renseignements personnels d'une organisation à une autre si les deux organisations sont soumises à un cadre de mobilité des données qui sera défini par voie réglementaire.

Les avantages vantés de la portabilité des données comprennent le renforcement du contrôle des particuliers sur leurs renseignements personnels et la stimulation de la concurrence en aidant à résoudre des problèmes tels que l'asservissement à un fournisseur et les obstacles à l'entrée des entreprises sur le marché[40].

Conformément au projet de loi C-11, le gouvernement a proposé l'élaboration de normes sectorielles et d'exigences techniques cohérentes pour faciliter le transfert de données entre les organisations de ce secteur. Le CIPVP soutient l'inclusion par la province d'un droit à la portabilité des données dans un cadre de protection de la vie privée du secteur privé, dans la mesure où il est interopérable avec celui d'autres instances et aide à faciliter le mouvement des données au-delà des frontières. Nous soutenons également une approche sectorielle pour l'élaboration de normes et d'exigences techniques qui garantiraient un cadre approprié et propre au contexte pour la portabilité des données.

À ce jour, certains experts ont indiqué que le droit à la portabilité des données a été sous-utilisé dans les instances qui l'ont introduit, en soulignant des problèmes tels que l'authentification correcte des utilisateurs, le traitement approprié des renseignements personnels de tiers, les risques et responsabilités juridiques si les données sont transférées à un fournisseur de services dont les protections en matière de confidentialité ou de sécurité sont faibles, la sécurité des données en transit et les risques de transferts ultérieurs ou d'autres utilisations en aval des données[41]. L'Ontario peut apprendre des modèles et de l'expérience de mise en œuvre d'autres territoires de compétence. Une approche progressive peut également contribuer à remédier aux faibles niveaux d'adoption constatés dans d'autres instances[42].

Le gouvernement sollicite également des commentaires sur la portée appropriée des dispositions relatives à la transférabilité. À notre avis, les dispositions de l'Ontario en matière de transférabilité devraient aller au-delà des seuls renseignements fournis par le particulier à l'organisation pour inclure d'autres données observées sur ce particulier (comme l'historique de recherche ou les données de localisation). Il existe des arguments pour et contre l'extension du droit à la portabilité aux données dérivées, telles que les profils de consommateurs et les prévisions comportementales. Nous comprenons que des particuliers peuvent souhaiter la portabilité de ce type de renseignements personnels, néanmoins, des facteurs concurrents de propriété et de confidentialité doivent être pris en compte. Le CIPVP se réjouit de s'engager avec le gouvernement et les autres intervenants concernés sur ces aspects plus granulaires d'un cadre de portabilité des données, y compris l'élaboration de règlements et de normes techniques propres au secteur.

VI. DISPOSITION ET DÉSINDEXATION

Dans son livre blanc, le gouvernement propose un droit de demander la disposition des renseignements personnels recueillis auprès de la personne, sous réserve d'exceptions limitées.

Notre bureau soutient le droit de disposition, surtout lorsque les renseignements sont fournis par le particulier ou sont observés au sujet de ce particulier. Si le droit de disposition est étendu à tous les renseignements personnels qu'une organisation détient sur une personne, quelle que soit leur source ou leur origine, il faudra travailler davantage pour définir les facteurs de perception de droits compensateurs au droit de disposition, en particulier lorsque les droits d'autres personnes garantis par la Charte peuvent être engagés.[43] La question de savoir si le droit des mineurs à disposer de leurs renseignements personnels pèse plus dans la balance en raison de leur vulnérabilité inhérente mérite également d'être examinée sérieusement.

Lorsqu'une organisation refuse la demande d'un particulier de détruire ses renseignements personnels, nous en convenons que l'organisation devrait être tenue de fournir à ce particulier les raisons de son refus et de l'information sur les recours possibles. Nous sommes également heureux de constater que l'obligation de disposition de l'organisation inclurait la responsabilité de s'assurer que tous les fournisseurs de services tiers qui ont reçu les renseignements personnels dans le cadre de la prestation d'un service à l'organisation doivent également les détruire.

Une question connexe, mais distincte est la nécessité d'envisager l'intégration d'une exigence de désindexation. La désindexation donne aux particuliers le droit de demander que certains contenus en ligne liés à leur nom soient supprimés des résultats renvoyés par un moteur de recherche. En fait, les renseignements restent en ligne, mais ils deviennent plus difficiles à trouver pour d'autres. Selon nous, le droit de demander la désindexation est un outil important pour les particuliers (surtout les enfants et les jeunes) pour gérer leur réputation en ligne et exercer un contrôle sur des renseignements potentiellement embarrassants, inexacts, périmés ou non pertinents.

En conséquence, nous recommandons l'adoption d'un système de désindexation, sur le modèle de la loi 64 du Québec, elle-même inspirée par le Règlement général sur la protection des données. Le projet de loi 64 propose d'accorder aux particuliers le droit de demander que les hyperliens attachés à leur nom soient désindexés lorsque la diffusion contrevient à la loi ou à une ordonnance judiciaire, ou lorsque la diffusion cause un préjudice grave à la réputation ou à la vie privée qui l'emporte clairement sur le droit du public d'être informé ou sur la liberté d'expression d'une personne, et que la demande ne dépasse pas ce qui est nécessaire pour prévenir le préjudice[44]. Afin de concilier ces derniers intérêts, des critères explicites doivent être pris en compte, notamment le fait que la personne soit une personnalité publique ou un mineur, le caractère actuel et exact de l'information, le caractère sensible de l'information et le contexte dans lequel l'information est diffusée, ainsi que le temps écoulé depuis la diffusion de l'information.

À notre avis, le projet de loi 64 représente un plan de désindexation réfléchi et bien équilibré que le gouvernement de l'Ontario devrait sérieusement considérer dans le contexte de sa propre loi sur la protection de la vie privée dans le secteur privé.

2. UTILISATION SÛRE DE LA PRISE DE DÉCISION AUTOMATISÉE

Le CIPVP se réjouit de l'attention portée par le gouvernement à l'établissement de règles pour une utilisation sûre et fiable de l'IA et de la prise de décision automatisée.

En juin 2021, le CIPVP a exposé sa position initiale sur l'IA dans sa réponse[45] à la consultation du gouvernement de l'Ontario sur le *cadre pour l'intelligence artificielle (IA) digne de confiance* destiné à l'utilisation de l'intelligence artificielle *par le gouvernement*. Une grande partie du raisonnement sous-jacent de notre soumission sur l'IA est également applicable dans le contexte du secteur privé, et nous recommandons au gouvernement d'examiner cette soumission en parallèle avec nos commentaires ci-dessous.

I. CHAMP D'APPLICATION DE L'INTERDICTION

Le livre blanc de l'Ontario définit la prise de décision automatisée comme incluant toute technologie qui « *assiste* ou remplace le jugement des décideurs humains »[46] (en italiques). Cette définition proposée semble s'inspirer du projet de loi C-11 et de la directive du gouvernement du Canada sur la prise de décision automatisée[47]. Il s'applique à un large éventail de techniques d'analyse de l'information[48], tant lorsque la prise de décision humaine est remplacée, ou assistée, par un tel système. Cela signifierait que les décisions entièrement automatisées et les décisions humaines qui sont simplement assistées par un processus automatisé seraient traitées de la même manière. Par conséquent, l'interdiction d'utiliser des systèmes de décision automatisés pour prendre des décisions susceptibles d'avoir de lourdes répercussions sur un particulier s'appliquerait aux deux types de décision.

En revanche, l'interdiction équivalente de l'article 22 du Règlement général sur la protection des données concerne les décisions fondées « uniquement sur un traitement automatisé ». En se concentrant *uniquement* sur les décisions automatisées, l'approche du Règlement général sur la protection des données incite les organisations à avoir une « intervention humaine ». L'intervention humaine fait en sorte (au moins lorsqu'une décision produit des effets juridiques concernant un particulier ou a de lourdes répercussions sur elle) qu'un décideur humain joue un rôle non négligeable dans le résultat et en assume la responsabilité.

La surveillance humaine n'est pas une panacée qui permet de remédier à tous les préjudices causés par les algorithmes[49]; elle n'en constitue pas moins une mesure de responsabilisation importante qui doit être encouragée. Si l'intention politique du gouvernement est d'inciter les organisations à introduire une intervention humaine, il pourrait envisager de restreindre l'interdiction contre la prise de décision automatisée

proposée *uniquement* pour les décisions automatisées, comme dans le *Règlement général sur la protection des données*.

D'autre part, si l'intention de la politique publique du gouvernement est d'accroître la transparence et le contrôle individuel en ce qui concerne *toute* décision susceptible d'avoir des répercussions importantes sur une personne, alors toute décision de ce type, quel que soit le moyen utilisé pour la prendre, devrait être soumise à tout ou partie des conditions[50] proposées pour les systèmes de décision automatisés.

Quelle que soit l'intention politique, il importe d'établir une correspondance nette entre cette intention et la loi proposée qui tient compte de la question de savoir si et quand des processus entièrement automatisés doivent être réglementés différemment du même processus réalisé avec une participation humaine pertinente.

II. EXCEPTIONS À L'INTERDICTION

Le livre blanc propose trois exceptions à l'interdiction d'utiliser des moyens automatisés pour prendre des décisions susceptibles d'avoir des répercussions importantes sur une personne : 1) une telle décision doit être nécessaire à la conclusion ou à l'exécution d'un marché entre l'organisation et le particulier; 2) une telle décision doit être autrement autorisée par la loi; ou 3) l'organisation obtient le consentement exprès du particulier.

Nous sommes heureux de constater l'intention du gouvernement de s'attaquer aux risques considérablement élevés pour la vie privée associés à l'IA. Par exemple, nous sommes d'accord avec la proposition d'exiger un consentement *explicite* lorsque le consentement est invoqué comme motif légitime pour une prise de décision automatisée. Cependant, nous craignons que les deux autres exceptions n'offrent pas réellement une protection accrue aux particuliers dont les renseignements personnels font l'objet d'une prise de décision automatisée par rapport à d'autres types de traitement.

Par exemple, l'exception de nécessité est très similaire à la première activité incluse dans la liste des activités commerciales qui seraient autorisées (sans consentement), mais elle n'est pas soumise aux mêmes garde-fous critiques qui s'appliquent à ces activités commerciales (voir notre discussion ci-dessous concernant les « *activités commerciales* »). De même, l'exception qui autoriserait la prise de décision automatisée, *si elle est autrement autorisée par la loi*, semblerait permettre aux organisations d'utiliser des moyens automatisés pour traiter des renseignements personnels en vertu de n'importe quel autre motif autorisé qui permet tout autre type de traitement.

Cela soulève la question suivante : de quelle manière une loi ontarienne pourrait-elle améliorer les protections à l'égard des particuliers qui peuvent être touchés de manière significative par les systèmes de décision automatisés? Nous recommandons que les exceptions à l'interdiction de la prise de décision automatisée soient renforcées en conséquence afin de fournir des protections plus significatives pour les individus

substantiellement touchés. Nous recommandons également d'envisager des protections supplémentaires, comme indiqué ci-dessous.

III. RESPONSABILITÉ, ÉVALUATION ET RÉVISION DES RISQUES

Les préjugés inhérents à un système de décision automatisé sont difficiles à détecter par l'analyse d'une seule décision. Au contraire, il faudra souvent analyser les résultats de nombreuses décisions (ainsi que les données connexes) avant de pouvoir commencer à dégager des tendances. Il serait donc inopportun de se fier exclusivement aux plaintes de particuliers qui font l'objet de ces décisions pour déterminer les préjugés dans un système déployé. L'évaluation et la détection de préjugés potentiels doivent commencer avant la mise en service d'un système et la surveillance du système doit être soutenue.

Lorsqu'une organisation prend des décisions automatisées qui ont de lourdes répercussions sur un particulier, elle devrait être tenue à une responsabilité en amont d'évaluer les effets algorithmiques de son système de décision automatisé. L'évaluation des effets algorithmiques devrait faire partie de son évaluation des facteurs relatifs à la vie privée (EFRVP) (voir la discussion ci-dessous). Un processus de diligence raisonnable devrait être engagé dès le début afin d'établir que des mesures raisonnables ont été prises pour cerner et atténuer les préjugés potentiels et pour évaluer et affirmer que les avantages potentiels du système ne sont pas contrés par des effets négatifs potentiels sur un particulier ou un groupe. Cette démarche devrait être complétée par un processus d'examen continu, tel qu'une évaluation des facteurs fondée sur des données probantes.

Conformément à une approche équitable, équilibrée, pragmatique, souple et proportionnée, il serait raisonnable d'accroître les exigences en matière de responsabilité et d'examen pour les systèmes de décision automatisés. L'accroissement des exigences devrait se faire en fonction de divers facteurs de risque tels que le volume, la nature et la sensibilité des renseignements concernées, les attentes raisonnables du particulier et les effets potentiels sur des particuliers ou groupes.

Nous recommandons que cette obligation générale de diligence raisonnable soit élaborée au moyen d'une réglementation et, si besoin, d'une orientation afin de fournir la flexibilité nécessaire pour garantir que ces divers facteurs de risque sont pris en compte de manière appropriée en fonction du contexte. Par exemple, dans certaines situations, l'évaluation des effets algorithmiques d'un système de décision automatisé peut nécessiter la participation de différentes unités opérationnelles de l'organisation afin de garantir la prise en compte de différents points de vue dans l'évaluation. Dans les situations impliquant des seuils de risque plus élevés, les organisations peuvent demander l'avis d'un organe externe de conseillers ou d'experts. Là où les risques sont encore plus élevés, il peut être nécessaire de consulter la ou les communautés les plus susceptibles d'être touchées par le système et, si besoin, de consulter un organe d'examen indépendant tel que le CIPVP, éventuellement.

Cette évaluation préalable au déploiement des systèmes de décision automatisés ne supprime pas la nécessité d'un examen continu des décisions après leur déploiement. Nous soutenons l'inclusion dans le livre blanc de mécanismes de contrôle solides, tels que la possibilité pour les particuliers de commenter et de contester une décision prise à leur sujet, de demander la correction des renseignements personnels utilisés pour rendre la décision et de faire examiner la décision.[51] Nous recommandons que les organisations soient tenues d'informer les particuliers de ces contrôles dans le cadre de l'obligation de l'organisation de répondre aux demandes d'explication du système décisionnel automatisé.[52]

IV. TENUE DE DOSSIERS

Le livre blanc invite à commenter la question des exigences appropriées en matière de tenue de dossiers. Nous recommandons — au minimum — que la tenue de dossiers efficace soit exigée pour toute décision automatisée qui affecte considérablement une personne. Il s'agirait notamment de documenter l'évaluation des risques réalisée à l'égard du système décisionnel automatisé adopté (voir la discussion ci-dessus).

Le livre blanc évoque la possibilité d'exiger « des organisations qu'elles consignent et retracent la collecte et l'utilisation des renseignements personnels » dans le contexte de prise de décision automatisée. Nous reconnaissons, comme le fait le livre blanc, que le fait d'exiger cela dans tous les cas pourrait potentiellement imposer un lourd fardeau aux organisations. Cependant, nous notons que, dans le cas de décisions automatisées qui se répercutent lourdement sur le particulier, le gouvernement propose (entre autres) de permettre au particulier de demander les renseignements personnels utilisés pour prendre la décision. En l'absence d'une obligation de tenue de dossiers, ce droit deviendrait théorique. Aussi recommandons-nous que cette exigence particulière en matière de tenue de dossiers soit soigneusement examinée à la lumière des avantages et des inconvénients.

V. RESTRICTIONS CONCERNANT LE PROFILAGE

Selon le livre blanc, des exigences ou des protections supplémentaires doivent être envisagées en ce qui concerne le profilage. Selon le livre blanc, « lorsque le profilage est à la base d'une décision qui affecte considérablement une personne, une fausse prédiction comporte un risque élevé de préjudice ». Cependant, un particulier peut être lésé par une prédiction *véridique* qui révèle des renseignements inconnus jusqu'alors, notamment en ce qui concerne des attributs de nature délicate (tels que des caractéristiques génétiques ou comportementales).

Compte tenu des risques de préjudice associés au profilage, nous recommandons de préciser que les profils des particuliers qui en découlent constituent également des renseignements personnels sur ces particuliers, qu'ils soient véridiques ou faux. En clarifiant explicitement ce point, les profils seraient soumis aux mêmes protections que tous les autres types de renseignements personnels, notamment l'accès, la correction, l'élimination, l'équité et le caractère approprié.

3. CONSENTEMENT RENFORCÉ

Le consentement joue un rôle central dans la loi canadienne sur la protection de la vie privée dans le secteur privé. Un cadre de consentement actualisé permettrait aux particuliers de s'attarder aux renseignements ayant le plus d'impact sur leurs décisions, tout en offrant aux organisations une plus grande souplesse pratique pour innover et être concurrentielles. Bien que, pour les raisons énoncées dans notre soumission précédente,[53] nous préférerions toujours un régime fondé sur le consentement en principe, sous réserve d'exceptions admissibles, nous commentons néanmoins l'approche que propose le gouvernement selon laquelle le consentement et les autres motifs de traitement des renseignements personnels sont d'égale importance.

I. CONSENTEMENT VALIDE

Dans l'ensemble, nous en convenons que les éléments d'information doivent être présentés en langage clair au moment ou avant le traitement présumé pour que le consentement soit jugé valide. Comme nous l'avons indiqué dans une soumission précédente, le consentement ne sera véritablement valable que s'il est raisonnable de s'attendre à ce que le particulier comprenne la nature, les fins et les conséquences de ce qui lui est demandé.

Nous appuyons l'ajout dans la liste des divulgations de renseignements d'une exigence selon laquelle le particulier doit être informé de son droit de donner, de refuser ou de retirer son consentement. Cet ajout relativement simple contribuera à rendre le consentement plus valable en faisant en sorte que les particuliers sachent qu'ils ont un véritable choix et qu'ils peuvent retirer leur consentement, sous réserve des exigences légales ou contractuelles applicables et d'un préavis raisonnable.

Enfin, et conformément à la *LPRPDE* et au projet de loi C-11, nous recommandons que toute loi ontarienne éventuelle interdise clairement aux organisations d'exiger, comme condition à l'offre d'un produit ou d'un service, qu'un particulier consente à la collecte, à l'utilisation ou à la communication de ses renseignements personnels au-delà de ce qui est nécessaire pour fournir le produit ou le service. De même, il devrait être interdit aux organisations d'obtenir le consentement par des moyens trompeurs ou frauduleux.

II. II. FORME DE CONSENTEMENT

En ce qui concerne la forme du consentement, selon le livre blanc, l'Ontario pourrait permettre aux organisations de s'appuyer sur un consentement implicite dans certaines circonstances, en tenant compte de la sensibilité des renseignements personnels en cause et des attentes raisonnables de la personne. Le CIPVP soutient la codification de ces conditions bien établies pour le consentement implicite.[54]

Nous recommandons de préciser plus explicitement que les mêmes exigences de divulgation de renseignements s'appliquent au consentement implicite qu'au consentement explicite, y compris l'obligation d'informer les particuliers de leur droit de retirer leur consentement. En outre, pour que le consentement implicite soit valable, les particuliers doivent disposer d'un moyen opportun et applicable d'exprimer leur objection au consentement (consentement par refus) et d'une possibilité permanente de retirer le consentement après coup, sous réserve des exigences juridiques ou contractuelles applicables et d'un préavis raisonnable.

III. ACTIVITÉS COMMERCIALES

L'une des mises à jour les plus importantes du modèle de consentement figurant dans les propositions de l'Ontario est la possibilité pour les organisations de recueillir et d'utiliser des renseignements personnels sans consentement dans le cadre d'activités commerciales normales, sous réserve de deux garde-fous importants : qu'une personne raisonnable s'attende à une telle collecte ou utilisation pour l'activité en question, et que les renseignements personnels ne soient pas recueillis ou utilisés dans le but d'influencer le comportement ou les décisions de la personne.

Nous convenons que ces deux garde-fous constituent des limites raisonnables au traitement de renseignements personnels sans consentement. En outre, il devrait être explicitement précisé que la collecte et l'utilisation de renseignements personnels dans le cadre d'activités commerciales autorisées restent assujetties à l'exigence primordiale selon laquelle elles doivent être effectuées à des fins qu'une personne raisonnable trouverait justes et appropriées dans les circonstances. L'établissement d'un lien avec la clause relative aux fins justes et appropriées fournirait le troisième garde-fou nécessaire pour garantir que ces activités commerciales (notamment « l'exercice d'une diligence raisonnable pour prévenir ou réduire les risques commerciaux de l'organisation ») sont menées de manière responsable et respectueuse en l'absence de consentement.

La proposition de l'Ontario relative aux activités commerciales a sensiblement retiré de sa liste ce qui, à notre avis, était l'une des dispositions les plus inquiétantes du projet de loi C-11, à savoir « une activité au cours de laquelle il serait impossible d'obtenir le consentement du particulier parce que l'organisation n'a pas de relation directe avec lui ». Nous appuyons sans réserve la suppression de cette activité commerciale d'une éventuelle loi.

Nous restons toutefois préoccupés par la possibilité d'élargir le champ des activités commerciales autorisées par voie de réglementation à une date ultérieure. En raison de cette disposition, de nouvelles activités commerciales peuvent être facilement ajoutées sans les importants contrôles et équilibres qui accompagnent le processus de modification législative. Nous recommandons de supprimer la possibilité d'activités prescrites de la liste des activités commerciales.

IV. TRANSFERT DE DONNÉES À DES FOURNISSEURS DE SERVICES AUX FINS DE TRAITEMENT

Compte tenu de la réalité pratique du fonctionnement et de la compétitivité de la plupart des entreprises dans un contexte commercial moderne, nous sommes favorables à l'autorisation proposée pour les organisations de transférer des renseignements personnels à des fournisseurs de services tiers sans exiger le consentement des particuliers dans chaque cas. Hormis les quelques réserves qui suivent, nous sommes d'accord avec la proposition de l'Ontario de permettre à une organisation de transférer les renseignements personnels d'un particulier à un tiers fournisseur de services aux fins de traitement et de permettre au fournisseur de services d'utiliser ces renseignements uniquement aux fins pour lesquelles ils lui ont été transférés.

Nous recommandons toutefois certaines améliorations. Premièrement, nous recommandons que le libellé de ces dispositions utilise le terme « transfert » de manière plus cohérente dans le contexte du traitement par un tiers, afin de distinguer ces types de transactions des cas de divulgations pures et simples. Deuxièmement, nous recommandons que l'organisation qui transfère des renseignements personnels à un fournisseur de services aux fins de traitement ne soit autorisée à le faire que si elle garde le contrôle des renseignements en s'assurant, entre autres, que le traitement est effectué en son nom et sous sa direction, et dans le même but légalement autorisé pour lequel les renseignements personnels ont été recueillis en premier lieu. Troisièmement, tant l'organisation que ses fournisseurs de services doivent être soumis à des exigences claires en matière de responsabilité, qui répartissent explicitement les responsabilités entre eux[55] (voir la section sur la responsabilité ci-dessous).

V. DIVULGATION À UN ORGANISME CHARGÉ DE L'EXÉCUTION DE LA LOI

Les dispositions permettant de divulguer des renseignements aux organismes chargés de l'exécution de la loi sans consentement existent généralement dans les lois canadiennes sur la protection de la vie privée. Cependant, à notre avis, le cadre actuel de l'Ontario concernant les divulgations proposées aux organismes chargés de l'exécution de la loi devrait être mieux défini afin de minimiser le risque d'incursions injustifiées dans les droits à la vie privée protégés par la Constitution.

La proposition actuelle permettrait aux organisations de divulguer des renseignements personnels à un organisme chargé de l'exécution de la loi au Canada 1) s'il y a des motifs raisonnables de croire qu'une violation a été commise *et* 2) que la divulgation permettrait à l'organisme d'établir s'il y a lieu de mener une enquête à ce sujet (l'accent est un ajout).

Par ailleurs, pour des raisons pratiques et à la lumière de notre expérience de l'interprétation de dispositions similaires dans le cadre des lois du secteur public, nous recommandons que la première condition de la disposition soit élargie pour permettre la

divulgation s'il existe des motifs raisonnables de croire qu'un crime est en train ou sur le point d'être commis.

D'autre part, nous recommandons de restreindre cette disposition de trois façons. Premièrement, pour éviter des divulgations trop larges, nous recommandons que la deuxième condition de la disposition soit restreinte pour n'autoriser la divulgation de renseignements personnels que dans la mesure où l'on peut raisonnablement penser qu'elle est *nécessaire* pour permettre à l'organisme chargé de l'exécution de la loi d'établir s'il doit mener une enquête. Deuxièmement, les termes « organisme chargé de l'exécution de la loi » et « enquête » doivent être définis de manière claire et étroite afin d'éviter une expansion indue de la disposition. Troisièmement, nous recommandons que la disposition soit clarifiée pour préciser que cette divulgation doit être à l'*initiative* de l'organisation plutôt qu'à la demande de l'organisme chargé de l'exécution de la loi.[56] Pour traiter les cas où la communication est demandée par l'organisme chargé de l'exécution de la loi, nous recommandons d'inclure une disposition distincte exigeant que l'organisme chargé de l'exécution de la loi définisse son autorité légitime et indique le motif de sa demande avant que la communication ne puisse être effectuée. Les articles 44 et 45 du projet de loi C-11 donnent un exemple de cette importante distinction entre la communication faite à la demande de l'organisme chargé de l'exécution de la loi et la communication sur l'initiative de l'organisation.

En définitive, comme nous le verrons dans la section sur la transparence, nous estimons qu'une future loi ontarienne devrait comporter des exigences de plus grande transparence en ce qui concerne les divulgations aux organismes chargés de l'exécution de la loi. De telles exigences de transparence permettraient au public de mieux comprendre la prévalence des organisations qui divulguent des renseignements personnels aux organismes chargés de l'exécution de la loi de l'ordre, notamment dans les cas de divulgations sans mandat.

VI. ENQUÊTE OU INSTANCE JUDICIAIRE

En vertu de cette disposition, une organisation peut recueillir, utiliser ou divulguer les renseignements personnels d'un particulier si cela est raisonnable aux fins d'une enquête ou d'une instance judiciaire. Selon nous, cette disposition est trop large et devrait être encadrée et circonscrite de manière appropriée afin d'éviter les atteintes injustifiées à la vie privée.

Nous recommandons que les termes « instance judiciaire » et « enquête » soient clairement définis. Nous recommandons que la disposition proposée soit divisée en deux ou plusieurs dispositions distinctes afin de définir les conditions qui s'appliquent à chaque cas.

Dans le cas des enquêtes, la loi doit préciser quel type d'enquête est censé être visé. Est-il destiné à des enquêtes relatives à la violation d'un accord ou à l'infraction à une loi? Est-il destiné à des enquêtes menées par l'organisation elle-même, un organisme d'enquête tiers désigné, ou une autre organisation? La loi devrait également renforcer considérablement

les conditions liées à cette collecte, cette utilisation ou cette divulgation. Comme dans le cas du projet de loi C-11, nous recommandons d'ajouter comme conditions que l'organisation ait des motifs raisonnables de croire qu'une violation d'un accord ou une infraction à une loi a été, est ou est sur le point d'être commise; que l'obtention du consentement d'une personne compromettrait probablement la disponibilité ou l'exactitude des renseignements; et que les renseignements sont raisonnables aux fins de l'enquête.

Pour ce qui est des instances judiciaires, nous recommandons que la disposition soit modifiée pour préciser, à l'instar du projet de loi C-11, que la divulgation de renseignements personnels peut se faire en vue de se conformer à une assignation délivrée, à une ordonnance rendue ou à une exigence semblable imposée dans une instance par une personne qui a compétence pour ordonner la production de renseignements ou en vue de se conformer à une règle de procédure relative à la production de renseignements dans une instance. (Voir l'alinéa 41(1)d) de la *LPRPS* pour un libellé similaire).

VII. RENSEIGNEMENTS PERSONNELS DES EMPLOYÉS

La proposition du gouvernement comprend de nouvelles protections pour la collecte, l'utilisation et la divulgation des renseignements des employés. Comme nous l'avons indiqué dans nos remarques préliminaires, le fait de combler les lacunes en matière de protection de la vie privée des employés serait une avancée majeure du droit à la vie privée en Ontario.

Dans la forme proposée, cependant, nous craignons que les nouvelles dispositions soient trop larges et permettent à un employeur de recueillir, d'utiliser et de divulguer des renseignements sur un employé dans la mesure où cela est raisonnable pour gérer la relation d'emploi. La *LPRPDE* et le projet de loi C-11 exigent que la collecte, l'utilisation et la communication soient nécessaires à l'établissement, à la gestion ou à la cessation de la relation d'emploi et que les employés soient informés des prétendues pratiques relatives aux renseignements. Nous demandons instamment au gouvernement d'introduire des exigences similaires de nécessité et de préavis dans une éventuelle loi ontarienne.

VIII. RECHERCHE DANS L'INTÉRÊT PUBLIC

La disposition proposée autorisant la recherche dans l'intérêt public est claire et habilitante, mais également soumise à un certain nombre de protections raisonnables de la vie privée. À notre avis, il s'agit d'une amélioration par rapport à la disposition équivalente qui existe actuellement dans la LPRPDE*,* qui, selon nos connaissances, a été considérablement sous-utilisée.

Toutefois, tel qu'il est actuellement proposé, le projet de disposition sur la recherche exigerait que la recherche *porte sur* l'intérêt public. Selon nous, cette condition devrait être renforcée afin de n'autoriser l'utilisation ou la divulgation non consensuelle des

renseignements personnels d'un particulier que lorsque les fins de la recherche sont censées *avancer* l'intérêt public.

IX. RENSEIGNEMENTS MIS À LA DISPOSITION DU PUBLIC

Selon le livre blanc, une organisation peut recueillir et utiliser les renseignements personnels d'un particulier sans son consentement si les renseignements personnels sont mis à la disposition du public et que la collecte est compatible avec les fins pour lesquelles et le contexte dans lequel les renseignements ont été mis à la disposition du public et les attentes raisonnables de la personne.

Le fait que des renseignements personnels puissent être accessibles en ligne ne signifie pas qu'un particulier n'a pas d'attente raisonnable en matière de respect de sa vie privée. Des cas récents, tels que l'enquête menée par les commissaires canadiens à la protection de la vie privée sur Clearview AI[57], mettent en évidence le risque que des organisations se livrent à un grattage massif et aveugle de l'Internet et extraient des renseignements personnels dans le but de les monnayer, souvent à l'insu des particuliers et en les exposant à des violations de la vie privée et à d'autres préjudices.

Nous sommes heureux de constater que la proposition du gouvernement concernant les renseignements personnels mis à la disposition du public comprend des exigences importantes selon lesquelles la collecte doit être compatible avec les fins pour lesquelles et le contexte dans lequel les renseignements ont été rendus accessibles au public et les attentes raisonnables du particulier. Toutefois, afin d'améliorer la protection de la vie privée des particuliers dans ce qui pourrait devenir une chasse ouverte aux renseignements personnels en ligne, nous invitons le gouvernement à envisager des critères supplémentaires inspirés de la définition de l'information accessible au public récemment adoptée dans la *Loi sur le Centre de la sécurité des télécommunications, L.C. 2019, ch. 13, art. 76,* notamment : information 1) publiée ou diffusée à l'intention du grand public, 2) accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, et 3) (surtout) à l'égard de laquelle un particulier *n*'a *aucune* attente raisonnable en matière de protection de la vie privée.

De plus, eu égard à l'objectif que s'est fixé le gouvernement en matière de politiques – qui est de protéger les populations vulnérables, et plus précisément les enfants et les jeunes –, nous recommandons que le gouvernement envisage sérieusement d'exclure explicitement de la définition de renseignements personnels accessibles au public tout renseignement affiché en ligne (plus précisément sur les sites Web de médias sociaux), permettant d'identifier un enfant ou un jeune. Le cas échéant, l'organisation qui voudrait utiliser des renseignements personnels d'enfants ou de jeunes ayant été affichés en ligne n'aurait pas carte blanche, et elle devrait invoquer un autre motif autorisé, par exemple un consentement ou la conduite de recherche dans l'intérêt public.

4. TRANSPARENCE DES DONNÉES POUR LES ONTARIENS

Comme nous l'avons énoncé dans notre mémoire présenté en octobre 2020, la transparence sera l'un des plus importants principes qui sous-tendront la loi moderne sur la protection de la vie privée dans le secteur privé, et elle sera également le pilier central de son succès. Les exigences en matière de transparence peuvent servir des objectifs multiples et distincts :

i. **Pour les particuliers**, ces exigences sont une composante essentielle pour assurer l'obtention d'un consentement éclairé à la collecte, l'utilisation et la divulgation de renseignements personnels;

ii. **Pour le grand public**, elles offrent une occasion essentielle de comprendre et de comparer les pratiques de gestion des données entre les concurrents d'un secteur donné;

iii. **Pour les organismes de réglementation et de surveillance**, elles offrent un outil permettant d'examiner en profondeur les pratiques d'une organisation afin d'en garantir la conformité et de tenir les organisations responsables.

En ce qui a trait aux renseignements qui doivent être communiqués aux particuliers au moment d'obtenir un consentement éclairé, ceux-ci doivent être relativement concis, opportuns et exploitables et être principalement axés sur les éléments les plus susceptibles d'éclairer les choix et les décisions de la personne. À ce sujet, veuillez consulter les commentaires que nous avons formulés précédemment sous « Consentement valide ».

En ce qui a trait au deuxième objectif précité – à savoir la diffusion des pratiques de gestion des données afin que le public puisse établir des comparaisons entre les organisations – nous appuyons la proposition formulée dans le livre blanc qui est d'exiger des organisations qu'elles fassent preuve de transparence quant à leurs pratiques de gestion des renseignements, que ces pratiques reposent sur l'obtention d'un consentement ou sur un autre motif autorisé.

À l'appui de ce deuxième objectif, nous croyons que les exigences en matière de transparence, qui sont énoncées à la page 29 du livre blanc, donnent un bon aperçu des renseignements généralement *utiles*, mais pas nécessairement exhaustifs, à fournir aux particuliers. Par exemple, bien qu'il soit utile pour le public de comprendre quelles données sont recueillies par l'organisation, la description de la source de ces données pourrait procurer une valeur ajoutée. De plus, de nombreux travaux sont en cours pour examiner des façons plus efficaces de communiquer de tels renseignements.[58] À cette fin, tout projet de loi devrait, tout au moins, être conçu de manière à offrir une certaine latitude quant à la liste des exigences générales en matière de transparence et aux nouvelles approches pouvant être utilisées pour assurer cette transparence, ceci afin de tenir compte de l'évolution de la recherche dans ce domaine.

Une autre exigence en matière de transparence, dont l'ajout serait bénéfique pour le public, serait d'exiger que les organisations publient des rapports publics annuels, présentant des statistiques de base sur le nombre et le type de demandes d'accès aux renseignements personnels détenus par ces organisations, que ces organisations ont reçues d'organismes chargés de l'application de la loi, et sur l'issue de ces demandes[59]. À l'échelle internationale, les autorités en matière de protection de la vie privée demandent depuis quelque temps déjà le renforcement de la transparence et de l'obligation de rendre compte, comme en témoigne notamment l'adoption d'une résolution[60] en ce sens lors de la 37e Conférence internationale des Commissaires à la protection des données et de la vie privée, qui s'est tenue en 2015. Ces rapports sur la transparence offrent de précieux outils pour veiller à ce que le gouvernement et les organismes chargés de l'application de la loi agissent de manière responsable et à ce que les organisations fassent preuve de diligence raisonnable dans le traitement des demandes de divulgation. Le contenu potentiel des rapports sur la transparence, et les politiques connexes en matière de divulgation, sont examinés dans la feuille-info du CIPVP de 2018 intitulée *Divulgation de renseignements personnels à un organisme d'exécution de la loi*[61], ainsi que dans les *Lignes directrices concernant la production de rapports sur les mesures de transparence*[62] du gouvernement du Canada.

Enfin, le troisième objectif de la transparence est de permettre aux organismes de réglementation et de surveillance de la vie privée (dans le cas présent, le CIPVP) de faire un examen minutieux des pratiques d'une organisation pour en garantir la conformité, d'évaluer les facteurs de risque systémiques et de tenir les organisations responsables de satisfaire à leurs obligations aux termes de la loi régissant la protection de la vie privée dans le secteur privé. Ces exigences en matière de transparence devraient notamment prévoir l'obligation, pour les organisations, de communiquer au CIPVP, sur demande, leurs politiques, pratiques et procédures en matière de protection de la vie privée; de fournir au CIPVP, sur demande, des statistiques annuelles sur les atteintes à la vie privée; de faire rapport au CIPVP en cas d'atteinte aux mesures de sécurité présentant un risque réel de préjudice important; de présenter les rapports des évaluations de l'impact sur la protection de la vie privée pour le traitement des données au-delà d'un seuil de risque défini (y compris les évaluations connexes de facteurs algorithmiques dont les effets sur des particuliers sont importants), ainsi que d'informer le CIPVP de l'intention d'une organisation d'utiliser ou de divulguer des renseignements personnels sans consentement pour mener des recherches dans l'intérêt public.

Il convient toutefois de préciser que de telles obligations en matière de transparence ne conféreraient pas une immunité aux organisations non conformes. Le CIPVP doit pouvoir donner suite aux renseignements qu'il reçoit et collaborer avec l'organisation concernée afin de résoudre les problèmes relevés et, s'il s'avère impossible de les régler (ou en cas de non-conformité évidente), de prendre des mesures coercitives.

I. ACCROÎTRE LA RESPONSABILITÉ

En plus des exigences de transparence imposées aux organisations pour *démontrer* aux organismes de réglementation qu'elles font preuve de responsabilité, s'ajoutent les obligations sous-jacentes relatives à la responsabilisation à proprement parler. La responsabilité fondamentale doit occuper une place centrale dans toute loi moderne sur la protection de la vie privée qui s'écarte d'un modèle entièrement fondé sur le consentement. Le renforcement des exigences en matière de reddition de compte vise à faire contrepoids à la plus grande marge de manœuvre dont bénéficient les organisations pour recueillir, utiliser ou divulguer des renseignements personnels sans consentement, dans une économie axée sur les données.

Bien que l'obligation pour les organisations de mettre en œuvre un programme modulable de gestion de la vie privée soit l'une des principales exigences fondamentales d'un cadre de responsabilisation 1.0, la loi moderne sur la protection de la vie privée doit prévoir des mesures de reddition de compte beaucoup plus rigoureuses, compte tenu des risques actuels et futurs croissants qui sont associés au numérique.

Nous recommanderions tout au moins d'imposer l'obligation de mener une évaluation de l'impact sur la protection de la vie privée (EIPVP) au-delà d'un certain seuil de risque; une telle évaluation devrait prévoir une évaluation de facteurs algorithmiques dans le cas de systèmes décisionnels automatisés qui touchent des particuliers de manière significative (voir nos commentaires ci-dessus). Cette exigence serait en principe conforme au Règlement général sur la protection des données (RGPD)[63]. Afin d'assurer une marge de manœuvre appropriée, nous recommanderions que les éléments requis de l'EIPVP soient prescrits par règlement ou qu'ils soient énoncés dans un document d'orientation afin de garantir l'utilisation d'une méthode systématique pour déterminer, évaluer, atténuer et gérer les risques pour les particuliers visés.

Nous ne proposerions pas que des EIPVP soient exigées pour *toute* collecte, utilisation et divulgation de renseignements personnels, car cela pourrait entraîner des frais administratifs importants qui pèseraient injustement sur les organisations. Cependant, lorsque la collecte, l'utilisation ou la divulgation présente des risques importants qui dépassent un certain seuil, une EIPVP serait alors exigée pour éviter que les frais et le fardeau en découlant soient injustement transférés aux particuliers qui devraient autrement soutenir tout le poids d'initiatives conçues à mauvais escient.

II. LA RESPONSABILITÉ DES FOURNISSEURS DE SERVICES

Une loi moderne sur la protection de la vie privée doit établir un régime clair et cohérent qui permet de répartir la responsabilité entre les multiples acteurs intervenant dans les accords complexes de traitement des données. Par conséquent, nous recommandons que toute loi proposée énonce clairement les obligations à la fois des organisations qui transfèrent les données et de leurs fournisseurs de services[64]. (Voir nos commentaires précités dans la section « Transferts de données aux fournisseurs de services à des fins de traitement ».)

L'organisation qui transfère légalement des renseignements personnels à un fournisseur de services tiers chargé de traiter les données en son nom devrait toutefois conserver le contrôle de ces renseignements personnels et demeurer ultimement responsable de ces données[65]. L'organisation qui transfère les données devrait notamment être tenue de garantir, aux termes d'un marché ou par un autre moyen, 1) que le fournisseur de services ne peut traiter les données que conformément à l'objectif légalement autorisé pour lequel il y a eu transfert et 2) que le fournisseur de services assurera un niveau de protection de la vie privée équivalant à celui que l'organisation est tenue d'offrir aux termes de la loi. Si le fournisseur de services est situé à l'extérieur de la province, comme c'est de plus en plus souvent le cas, l'obligation, pour l'organisation qui transfère les données de divulguer ce fait et de fournir une description des risques et conséquences connexes, devrait faire partie de ses obligations en matière de transparence. L'organisation qui transfère les données devrait également conserver la responsabilité de répondre aux demandes d'accès ou d'élimination, et celle d'informer les particuliers visés ou de faire rapport au CIPVP en cas d'atteinte à la protection des données.

Il devrait par ailleurs être interdit aux fournisseurs de services d'utiliser ou de divulguer des renseignements personnels à des fins autres que celle pour laquelle l'organisation leur a transféré les données à des fins de traitement. Les fournisseurs de services devraient également être tenus d'offrir le même niveau de protection que celui auquel l'organisation qui leur a transféré les données est assujettie. Les fournisseurs de services devraient aussi être tenus, de manière générale, de transmettre les demandes d'accès ou d'élimination à l'organisation concernée, d'informer immédiatement l'organisation en cas de violation des données et de collaborer avec l'organisation aux enquêtes sur ces incidents ainsi qu'aux mesures visant à en atténuer et en contenir les effets. Ces exigences générales devraient être énoncées dans la loi proprement dite, ainsi que, s'il y a lieu, dans des règlements d'application ou des documents d'orientation, afin de définir de manière plus précise les éléments devant faire partie de tout accord contractuel entre l'organisation et le fournisseur de services.

5. PROTÉGER LES ENFANTS ET LES JEUNES

Nous applaudissons à la proposition du gouvernement d'aborder, dans la loi sur la protection de la vie privée dans le secteur privé, des enjeux importants, tels que les mandataires spéciaux et les seuils d'âge minimum pour l'obtention d'un consentement en ligne valide.

Parallèlement, nous croyons qu'une approche équilibrée reconnaîtrait que les souhaits d'un jeune ne correspondent pas toujours à ceux de ses parents. Par exemple, de jeunes adolescents pourraient ne pas être d'accord avec la demande de leurs parents d'accéder à des renseignements personnels qu'ils ont publiés à leur propre sujet pour s'exprimer sur des médias sociaux, ou à des demandes visant à retirer ces renseignements. Inversement, des adolescents pourraient s'opposer à ce que leurs parents publient en ligne des photos ou d'autres renseignements personnels les concernant. Pour ces raisons et d'autres

encore, nous recommanderions qu'une loi sur la protection de la vie privée dans le secteur privé reconnaisse le droit de mineurs matures âgés de 13 à 16 ans de s'opposer au consentement de leurs parents ou aux demandes de leurs parents faites en leur nom, et que cette opposition ait préséance.

De plus, conformément aux opinions que nous avons exprimées précédemment, les jeunes devraient disposer du droit général de demander, même sans le consentement de leurs parents, que des renseignements qui ont été publiés à leur sujet soient désindexés, retirés et, dans certains cas, supprimés à la source[66], sous réserve d'exceptions limitées. Il s'agit d'une proposition que nous avons énoncée dans notre mémoire initial, dans lequel nous recommandions d'accorder une attention particulière aux mineurs afin de soutenir leur liberté d'expérimentation et de découverte de soi, et leur capacité d'apprendre et de changer d'avis à un jeune âge, sans craindre les effets permanents sur leur réputation que pourraient avoir des renseignements qu'ils publient en ligne à leur propre sujet.

Enfin, le gouvernement a proposé d'élaborer des codes de pratique supplémentaires qui ressembleraient à ceux mis en place ailleurs dans le monde. Au Royaume-Uni, par exemple, le bureau du commissaire à l'information a produit un code strict[67] dans ce domaine, qui cherche à protéger les enfants dans le monde numérique, mais non à les en protéger[68]. Le CIPVP appuie la proposition du gouvernement et serait heureux de participer à l'élaboration d'un code de pratique semblable pour l'Ontario, afin d'accroître la spécificité de la protection des enfants en ligne.

6. UN RÉGIME RÉGLEMENTAIRE ÉQUITABLE, PROPORTIONNÉ ET FAVORABLE

I. SOUTIEN PROACTIF

i. Codes de pratique et programmes de certification

L'une des questions que les intervenants posent le plus souvent aux organismes de réglementation de la protection de la vie privée est la suivante : « Que devons-nous faire pour nous conformer à la loi? ». Bien que nous cherchions à apporter un soutien par la tenue de consultations, nous voyons un grand potentiel dans la diffusion de documents d'orientation proactifs et plus détaillés, par l'élaboration concertée de codes de pratique et de programmes de certification. Les codes de pratique peuvent procurer de nets avantages aux Ontariens (qui, grâce à ces aide-mémoire, bénéficient d'une plus grande transparence de la part des organisations quant aux pratiques qu'elles utilisent), ainsi qu'aux organisations elles-mêmes (qui obtiennent ainsi une certaine certitude réglementaire quant à leurs propres pratiques et qui peuvent collaborer de manière plus sécuritaire avec des fournisseurs de services et des partenaires accrédités en regard de ces codes).

Bien sûr, l'approbation réglementaire d'un code, de toute modification qui y serait apportée, ainsi que de tout programme de certification de tiers mis en place pour

assurer la surveillance continue des organisations déclarant s'y conformer, nécessiterait l'établissement d'exigences rigoureuses (comme le prévoient le RGPD européen[69] et le projet de loi C-11[70]). Dans la mesure où ils sont compatibles, la loi ontarienne proposée pourrait aussi prévoir la reconnaissance réciproque des codes de pratique et des programmes de certification approuvés par l'organisme de réglementation fédéral, et vice versa. Il est toutefois important de souligner que l'adhésion à un code et à un programme de certification ne doit pas entraver l'exercice du pouvoir discrétionnaire de l'organisme de réglementation. Bien que le respect d'un code de pratique ou l'obtention d'une certification soit utile pour évaluer l'observation de la loi, il ne s'agit pas de facteurs déterminants du respect de la loi. Le CIPVP doit toujours conserver le pouvoir résiduel d'évaluer l'application de la loi en regard des faits et circonstances propres à chaque plainte, de tout changement ou écart par rapport aux pratiques ou aux politiques de l'organisation, ainsi que de tout risque nouveau.

ii. Régimes de réglementation souples

Comme nous l'avons mentionné dans notre précédent mémoire, nous encouragerions également le gouvernement à envisager l'adoption d'outils de réglementation avant-gardistes et souples, qui sont actuellement à l'essai par d'autres administrations.

Le principal exemple est le « bac à sable réglementaire », un environnement sûr et supervisé, à l'intérieur duquel les organisations peuvent mettre à l'essai et tester, sous la supervision de l'organisme de réglementation de la vie privée, des produits et des services novateurs pour s'assurer qu'ils sont conformes à la loi et à d'autres exigences. Cette approche a notamment été adoptée par le bureau du commissaire à l'information[71] du Royaume-Uni, l'Autorité norvégienne de protection des données[72] (plus précisément en matière d'IA) et la Commission de l'énergie de l'Ontario[73]. Là encore, l'objectif global serait de fournir à l'organisme de réglementation des moyens souples et modernes de soutenir, à l'intérieur d'un environnement sécurisé et supervisé, une innovation *conforme et respectueuse de la vie privée* de la part des organisations ontariennes.

iii. Documents d'orientation et conseils

Nous appuierions un éventail d'outils visant à favoriser et à encourager le respect de la réglementation qui s'ajoute aux mesures d'application de la loi prévues dans une loi sur la protection de la vie privée dans le secteur privé. De tels outils comprendraient notamment du matériel pédagogique, tels que des documents d'orientation et des pratiques exemplaires pratiques, transparents et exhaustifs, élaborés en consultation et en collaboration avec des organisations et des particuliers. Comme l'a souligné le gouvernement, le CIPVP publie depuis longtemps des documents d'orientation sur les lois que nous administrons[74]. Parmi les autres outils envisagés, mentionnons la prestation de services consultatifs sur les nouvelles formes de traitement de données, ainsi que le financement et la publication de recherches dans des domaines comportant des risques nouveaux.

Cependant, tout comme les codes et les programmes de certification, ces outils ne peuvent entraver l'exercice du pouvoir discrétionnaire du CIPVP dans l'évaluation du respect de la loi. Bien que les documents d'orientation, les conseils, les recherches et autres ressources soient d'importantes sources d'information à prendre en compte, les plaintes de particuliers devront continuer à être évaluées en fonction de l'application de la loi aux faits et aux circonstances propres à l'affaire, de tout changement ou écart par rapport aux pratiques ou politiques de l'organisation et de tout risque nouveau. De plus, afin d'assurer une affectation judicieuse des ressources, de se concentrer sur les domaines où le risque systémique est le plus élevé et d'offrir une valeur généralisable à l'ensemble des organisations d'un secteur ou d'une industrie, le CIPVP devrait avoir le pouvoir discrétionnaire de déterminer les orientations, conseils ou recherches à entreprendre. À cet égard, nous formulerions une mise en garde contre l'approche préconisée dans le projet de loi C-11[75], qui exige que le commissaire à la protection de la vie privée fournisse des conseils aux organisations qui le demandent, ce qui pourrait créer un avantage concurrentiel injuste sur le marché et drainer indûment les ressources publiques sans générer un grand retour sur investissement.

II. RÉGIME D'APPLICATION DE LA LOI

Le CIPVP est largement en faveur du cadre d'application de la loi qui est envisagé par le gouvernement, en vue de l'adoption d'une loi ontarienne sur la protection de la vie privée dans le secteur privé. Les options d'application de la loi visent plus particulièrement à combler quelques-unes des plus importantes lacunes du projet de loi C-11, ainsi qu'à donner suite à bon nombre des recommandations formulées par le CIPVP dans son précédent mémoire sur la loi ontarienne sur la protection de la vie privée dans le secteur privé.[76]

i. Pouvoirs de mener des enquêtes et de rendre des ordonnances

Le paysage moderne de la protection de la vie privée exige qu'un organisme de réglementation soit doté de vastes pouvoirs pour mener des enquêtes et rendre des ordonnances. Le CIPVP se réjouit que le gouvernement reconnaisse ce fait et qu'il envisage un modèle législatif qui confère au CIPVP le pouvoir de rendre des ordonnances obligeant les organisations à se conformer à la loi, à cesser d'y contrevenir, à rendre publiques les mesures qu'elles ont prises pour s'acquitter de leurs obligations, ainsi qu'à détruire tout renseignement personnel obtenu illégalement.

Le pouvoir de rendre des ordonnances doit être soutenu par des pouvoirs d'enquête robustes, mais souples. Le CIPVP doit avoir le pouvoir d'ouvrir une enquête de sa propre initiative ou en réponse à une plainte. Pour s'assurer que les ressources sont affectées, comme il se doit, aux questions les plus urgentes, le CIPVP doit également avoir le pouvoir discrétionnaire de déterminer quelles affaires devraient faire l'objet d'une enquête et quelles enquêtes devraient être abandonnées. Le CIPVP se réjouit que le gouvernement reconnaisse l'importance de lui accorder ce pouvoir discrétionnaire.

Bien que le CIPVP soutienne largement le modèle d'application de la loi à l'étude par le gouvernement, nous recommanderions que quelques améliorations précises y soient apportées. Premièrement, le pouvoir de rendre des ordonnances ne devrait pas se limiter uniquement relativement aux « organisations », mais devrait également s'appliquer relativement aux fournisseurs de services afin de s'assurer qu'eux aussi s'acquittent de leurs obligations prévues dans la loi proposée et ses règlements d'application (voir nos recommandations précitées, dans la section « Transferts de données aux fournisseurs de services à des fins de traitement »).

Deuxièmement, les ordonnances du CIPVP relativement aux droits d'accès aux données, ainsi qu'aux droits de mobilité, d'élimination, de désindexation et de rectification des données, ne devraient pas pouvoir faire l'objet d'appels devant les tribunaux, mais être plutôt soumises à un contrôle judiciaire. Ces modifications rendraient la loi proposée plus pratique, plus efficace et plus cohérente avec les autres lois administrées par le CIPVP[77] et contribueraient à garantir que les ordonnances rendues par le CIPVP relativement à ces droits ont un degré supérieur de certitude et de finalité.

ii. Sanctions administratives pécuniaires

La réglementation du secteur privé doit reconnaître la valeur économique des renseignements personnels, tout en créant des incitatifs financiers efficaces pour encourager le respect de la loi et éviter que des organisations profitent de l'inobservation de la loi. L'application de sanctions administratives pécuniaires est l'un des moyens de créer de tels incitatifs financiers. Le CIPVP est en faveur de l'introduction d'un régime de sanctions administratives pécuniaires dans le cadre d'une loi ontarienne sur la protection de la vie privée dans le secteur privé. Nous convenons également que les sanctions administratives pécuniaires devraient être imposées par le CIPVP, plutôt que par un tribunal administratif distinct comme celui proposé dans le projet de loi C-11.

Nous sommes d'avis que les dispositions proposées en matière de sanctions administratives pécuniaires assurent dans l'ensemble un bon équilibre. Ces dispositions se comparent à celles prévues dans la LPRPS de l'Ontario, tout en étant adaptées au secteur privé. Les propositions accordent également au CIPVP, à juste titre, le pouvoir discrétionnaire d'imposer ou non une sanction administrative pécuniaire, et elles définissent à cette fin une liste de facteurs à prendre en compte.

Bien que le CIPVP soutienne largement le modèle proposé par le gouvernement, nous recommandons plusieurs améliorations. Premièrement, le projet de dispositions limite les sanctions administratives pécuniaires aux seules « organisations ». Selon nous, les sanctions administratives pécuniaires devraient également s'appliquer aux fournisseurs de services dans les cas qui le justifient. Compte tenu de l'importance de leurs responsabilités en matière de traitement des données, nous recommandons qu'ils soient aussi couverts par une éventuelle loi (voir nos recommandations ci-dessus, « Transferts de données aux prestataires de services pour traitement »).

Deuxièmement, la disposition relative aux sanctions administratives, telle qu'elle est proposée, ne s'appliquerait qu'aux contraventions à la loi. La loi ontarienne sur la protection de la vie privée dans le secteur privé devrait garantir de manière cohérente que les infractions aux règlements peuvent également entraîner des sanctions administratives pécuniaires[78].

Troisièmement, nous recommandons que le montant maximal d'une sanction administrative pécuniaire pour une organisation qui est un particulier soit porté à 100 000 $. Si 50 000 dollars peuvent constituer une lourde pénalité pour de bien des particuliers, il est improbable que cela arrive à dissuader les comportements qui visent à tirer des avantages économiques bien supérieurs à 50 000 dollars en cas grave de non-conformité. D'autre part, le CIPVP convient que le montant maximum proposé pour une organisation qui n'est pas un particulier est approprié, tout en reconnaissant que les montants indiqués sont des maximums et que la détermination du montant réel d'une sanction administrative pécuniaire sera basée sur les faits et circonstances propres à chaque affaire.

Quatrièmement, les facteurs à prendre en considération pour décider de l'imposition d'une sanction administrative pécuniaire devraient être élargis pour tenir compte du fait qu'une sanction ou une amende a déjà été imposée en vertu d'autres lois sur la protection de la vie privée et l'accès à l'information relativement aux mêmes faits et circonstances. Cela permettra d'assurer l'interopérabilité de la législation ontarienne et des autres législations canadiennes en matière d'accès et de protection de la vie privée, de sorte que les organisations ne soient pas trop (ou injustement) pénalisées financièrement.

iii. Infractions

Le CIPVP est tout à fait d'accord qu'une loi ontarienne sur la protection de la vie privée dans le secteur privé devrait inclure un régime d'infractions statutaires. Cet outil d'application est un instrument important pour sanctionner les contraventions flagrantes tout en les dissuadant de se produire en premier lieu.

Nous sommes généralement d'accord avec les exemples d'infractions proposés dans le livre blanc, notamment lorsqu'une organisation réidentifie des renseignements personnels qui ont été dépersonnalisés; cherche à se venger d'un dénonciateur; omet de signaler au CIPVP une violation des mesures de sécurité; omet de tenir un registre de chaque violation des mesures de sécurité; omet de conserver des renseignements faisant l'objet d'une enquête du CIPVP; ou omet de se conformer à une ordonnance de conformité du CIPVP. Outre ces exemples, nous recommandons l'inclusion des infractions suivantes :

- Recueillir, utiliser ou divulguer volontairement des renseignements personnels en violation de la loi[79];
- Faire volontairement une fausse déclaration pour induire ou tenter d'induire en erreur le commissaire dans l'exercice de ses fonctions en vertu de la loi[80];
- Faire une fausse demande d'accès, de correction, de portabilité, d'élimination ou de désindexation ou concernant les systèmes de décision automatisés[81];

- Altérer, dissimuler ou détruire des renseignements personnels ou amener une personne à le faire dans l'intention de lui refuser un accès direct à la loi[82];
- Licencier, suspendre, rétrograder, discipliner, harceler ou désavantager de toute autre manière une personne qui a) a divulgué une violation de la vie privée au commissaire; b) a fait quelque chose d'exigé par la loi ou ses règlements; c) a refusé de faire quelque chose que la loi ou ses règlements interdisent[83].

L'inclusion de ces dispositions permettra de s'assurer que certaines des pires infractions à la législation ontarienne sur la protection de la vie privée dans le secteur privé constituent des infractions punissables, conformément à leur traitement en vertu d'autres lois ontariennes sur la protection de la vie privée, comme la *LPRPS*.

Nous notons également que les dispositions relatives aux infractions prévues dans le livre blanc ne s'appliquent qu'aux organisations. Conformément aux autres lois ontariennes sur la protection de la vie privée84, les dispositions relatives aux infractions devraient aller au-delà des organisations et s'appliquer à toute personne. En outre, nous recommandons que l'amende maximale pour des particuliers reconnus coupables d'une infraction soit plus faible que les amendes proposées pour des non-particuliers.

iv. Pouvoir d'ordonner une indemnisation

Une question soulevée dans le livre blanc est de savoir si le CIPVP devrait avoir la capacité d'ordonner que des particuliers soient indemnisés en cas de violation de leur vie privée. À notre avis, lorsque des particuliers ont été touchés par une violation, il pourrait y avoir un processus simplifié pour obtenir un niveau d'indemnisation de base tenant compte de la nature globale des risques créés par la contravention. À cet égard, le CIPVP pourrait avoir la possibilité de rendre une ordonnance exigeant le versement de montants discrets en indemnisation. Par exemple, le CIPVP peut ordonner que des services de surveillance du crédit et de protection contre le vol d'identité soient fournis aux particuliers touchés par une violation de la vie privée ou que les coûts d'annulation ou de résiliation prématurée d'une relation contractuelle avec l'organisation soient supprimés.

À l'aide de ses processus de résolution précoce et à ses efforts de médiation fondés sur les intérêts, le CIPVP pourrait amener les parties à une résolution mutuellement satisfaisante qui pourrait inclure une modeste indemnité financière unique à chaque particulier visé, évitant ainsi la nécessité d'une enquête et d'une éventuelle ordonnance.

Cependant, bien que le CIPVP soit particulièrement bien placé pour évaluer la nature générale d'une violation, les risques généraux créés pour les particuliers concernés et les mesures d'atténuation appropriées, nous ne sommes pas particulièrement bien placés pour évaluer les dommages individuels. Les demandes individuelles de dommages et intérêts doivent être traitées par les tribunaux.

En conséquence, les demandes individuelles d'indemnisation doivent être traitées en garantissant la disponibilité d'un droit privé d'action en dommages et intérêts lorsque le CIPVP constate une infraction à la loi ou qu'une personne a été condamnée pour une infraction à la loi[85].

7. SOUTIEN AUX INNOVATEURS DE L'ONTARIO

I. RENSEIGNEMENTS DÉPERSONNALISÉS

i. Utilisation autorisée des renseignements dépersonnalisés

Comme indiqué dans le livre blanc, le schéma de dépersonnalisation proposé est conforme à celui que propose le CIPVP dans une soumission antérieure à la consultation du gouvernement sur la protection de la vie privée dans le secteur privé. D'une manière générale, le système définit un seuil à partir duquel les renseignements sont considérés comme « dépersonnalisés » – toujours soumis à la législation sur la protection de la vie privée, mais bénéficiant d'une plus grande souplesse d'utilisation dans certaines situations définies. Il définit également les « renseignements anonymisés », qui seraient en dehors des quatre coins de la loi.

ii. Définition des renseignements dépersonnalisés

L'identifiabilité des renseignements peut être comprise comme étant le long d'un spectre. Dans un modèle binaire, ce spectre est divisé en « renseignements personnels », qui sont identifiables, et en « renseignements non personnels », qui ne le sont pas. Il n'y a cependant pas de frontière statutaire nette entre ces deux états. Les interprétations floues de l'identifiabilité par les organisations ont pour conséquence que les pratiques risquées de gestion de l'information passent complètement inaperçues ou, à l'inverse, que la réticence risque d'entraver une concurrence loyale et une innovation saine. Des tentatives pour aider les organisations à faire la distinction entre ces deux états de renseignements ont été entreprises par l'intermédiaire d'orientations, de réglementations, de codes de pratique et des tribunaux.

L'Ontario a proposé un modèle à trois états : renseignements personnels, renseignements dépersonnalisés et renseignements anonymisés. Bien que les « renseignements personnels » ne soient pas définis dans le livre blanc, on peut supposer qu'ils prendraient le sens universellement accepté de « renseignements concernant un particulier identifiable » (voir nos commentaires à la section « Définitions des renseignements personnels et des renseignements personnels sensibles »). La proposition définit les « renseignements dépersonnalisés » comme « des renseignements concernant un individu qui ne permettent plus de les identifier directement ou indirectement sans utiliser d'autres renseignements ». La définition proposée des « renseignements anonymisés » serait « des renseignements qui ont été modifiés de manière irréversible, selon les meilleures pratiques généralement acceptées, de telle sorte qu'aucun particulier ne puisse être identifié à partir de ces renseignements, que ce soit directement ou indirectement par quelque moyen ou par quelque personne que ce soit ».

Étant donné que les obligations d'une organisation différeraient en ce qui concerne chacun de ces trois états, il est essentiel que ces derniers soient bien définis. À cette fin, nous

recommandons que l'état intermédiaire des « renseignements dépersonnalisés » soit défini comme suit :

> « Les **renseignements dépersonnalisés** désignent les renseignements qui ne permettent pas d'identifier un particulier ou qui ne pourraient pas être utilisés dans des circonstances raisonnablement prévisibles, seuls ou en combinaison avec d'autres renseignements, pour identifier un particulier, mais qui présentent toujours un risque résiduel, aussi minime soit-il, de réidentifier un particulier »

L'ajout d'un seuil – à savoir les « circonstances raisonnablement prévisibles » – permet de mettre en place des mécanismes de gouvernance appropriés (physiques, techniques et administratifs), internes ou externes à une organisation, afin de séparer efficacement et en toute sécurité les données dépersonnalisées de tout autre renseignement susceptible d'être combiné et utilisé pour réidentifier une personne.

L'insertion de la clause finale évoquant le « risque résiduel, quoique minime, de réidentification d'une personne » vise à mieux différencier les renseignements dépersonnalisés des renseignements anonymisés, en aidant les organisations à déterminer plus clairement quand les renseignements restent soumis à la loi ou tombent en dehors de la loi et en permettant une approche plus cohérente de la dépersonnalisation entre les secteurs[86] et les instances[87].

Quant aux données anonymisées, beaucoup pourraient faire valoir que cet état des données est illusoire et que les renseignements personnels ne pourraient plus jamais être véritablement anonymes[88]. Bien que cela soit de plus en plus vrai à la lumière de l'évolution des technologies de l'information et de la quantité omniprésente de renseignements personnels largement disponibles en ligne, il reste certaines formes de données statistiques qui sont agrégées à un niveau suffisamment élevé pour permettre leur utilisation ultérieure et leur diffusion publique sans aucun risque de réidentification[89]. En outre, le fait de prévoir des données anonymisées laisse la possibilité à certaines technologies émergentes de renforcement de la vie privée (p. ex., les données synthétiques) d'atteindre ou de retrouver cet état d'anonymat, ce qui permet de les utiliser plus librement à des fins novatrices tout en présentant un risque effectivement nul pour les particuliers[90].

iii. Application

Nous soutenons fermement l'idée de faire entrer les renseignements dépersonnalisés dans le champ d'application d'une législation sur la protection de la vie privée dans le secteur privé. Toutefois, nous soulignons qu'il est important de le faire de manière explicite. Nous recommandons que cela soit fait dans la section d'application de la loi proposée.

Pour plus de clarté et pour faciliter l'interprétation, cette section pourrait énumérer les sections qui continuent ou non à s'appliquer aux données dépersonnalisées. Au minimum (et sous réserve de toute exception ciblée nécessaire), nous recommandons que les données dépersonnalisées restent soumises aux dispositions relatives à la responsabilité de l'organisation, aux objectifs justes et appropriés, aux garanties, à l'ouverture et à

la transparence, ainsi qu'à la possibilité de porter plainte à l'égard du non-respect des principes. Les dispositions que nous recommandons d'appliquer aux renseignements dépersonnalisés devraient également faire l'objet de mesures d'exécution appropriées en cas de non-respect.

Nous recommandons également qu'une loi ontarienne incite les organisations à dépersonnaliser les données autant que possible. Par exemple, lorsque la dépersonnalisation est utilisée comme mesure de sauvegarde, il pourrait s'agir d'une considération de diligence raisonnable ou d'un facteur d'atténuation lors de l'évaluation de la conformité et de l'application des mesures d'exécution de manière plus générale. En outre, la loi devrait préciser que les organisations sont autorisées à utiliser ou à divulguer des données dépersonnalisées dans toutes les circonstances où elles sont autorisées à utiliser ou à divulguer les renseignements personnels originaux à partir desquels les données dépersonnalisées ont été générées.

En ce qui concerne la disposition proposée demandant l'application de mesures techniques et administratives proportionnées aux données dépersonnalisées, nous sommes à l'aise avec l'approche fondée sur le risque qui tient compte de la finalité pour laquelle les renseignements sont dépersonnalisés et de la sensibilité des renseignements personnels. Pour plus de clarté, nous recommandons d'ajouter la prise en compte du contexte ainsi que des risques de réidentification.

Nous soutenons fermement la création d'une interdiction d'utiliser ou de tenter d'utiliser des renseignements dépersonnalisés dans le but de réidentifier un particulier (sous réserve d'exceptions étroites), ainsi que l'infraction connexe pour avoir sciemment enfreint une telle interdiction.

Enfin, nous recommandons de préciser les exigences de transparence concernant l'utilisation des renseignements dépersonnalisés *et* anonymisés. Selon la proposition actuelle, les organisations seraient tenues de fournir un « compte rendu général » de leur utilisation des renseignements dépersonnalisés. Selon nous, le fait de simplement déclarer que les renseignements seront « dépersonnalisés et utilisés pour la recherche et le développement internes » ou « à des fins socialement bénéfiques » ne répondrait probablement pas à l'intention politique d'atteindre une transparence significative. Les particuliers dont les renseignements personnels seront dépersonnalisés pour servir ces autres objectifs ont le droit de savoir quels sont ces objectifs, surtout lorsqu'il existe des risques résiduels de réidentification. À l'instar des investisseurs qui évitent de placer leur argent dans des fonds d'investissement qui ne correspondent pas à leurs valeurs éthiques, les particuliers devraient pouvoir savoir ce qui sera fait de leurs renseignements personnels et avoir au moins la possibilité, dans la mesure du possible, d'éviter les organisations qui se livrent à des pratiques qu'ils jugent répréhensibles. Les détails supplémentaires qui seraient nécessaires pour satisfaire ce niveau de transparence pourraient probablement être établis par l'intermédiaire d'orientations.

Un argument similaire en faveur d'exigences générales de transparence pourrait être avancé en ce qui concerne les renseignements anonymisés qui sont dérivés des renseignements personnels des particuliers à la source. Toutefois, cette question nécessite

une réflexion plus approfondie, car il est vrai que les renseignements anonymisés présentent un intérêt moindre, voire inexistant, pour la protection de la vie privée. En outre, la définition proposée des renseignements anonymisés – en tant que renseignements auxquels la loi ne s'appliquerait pas – devrait être ramenée dans le champ d'application de la loi dans le seul but de l'exigence de transparence.

Pour favoriser la « transparence à l'égard du régulateur », nous recommandons également que les organisations soient obligées de conserver des enregistrements de leur processus de dépersonnalisation. Cela pourrait faire partie d'une EFVP qui serait mise à la disposition du régulateur sur demande. Plus précisément, au-delà d'un certain seuil de risque, lorsque les données d'origine à partir desquelles les renseignements dépersonnalisés ont été dérivés sont sensibles ou que l'utilisation prévue peut avoir de lourdes répercussions sur les particuliers, une organisation doit clairement documenter les mesures qu'elle a prises pour dépersonnaliser les données, la base sur laquelle elle estime que ces mesures sont suffisamment efficaces et les raisons pour lesquelles elle pense raisonnablement que les objectifs de la recherche ou de l'innovation sont justes et appropriés. Cette exigence de transparence créerait une visibilité importante pour les régulateurs et une diligence raisonnable pour les organisations.

II. AUTRES MOYENS POTENTIELS DE SOUTENIR LES INNOVATEURS

En ce qui concerne la dernière question relative aux garanties ou aux modèles de gouvernance permettant le partage de renseignements dépersonnalisés à des fins socialement bénéfiques, il s'agit d'un domaine que nous continuons d'étudier et sur lequel nous avons l'intention de développer davantage notre position et nos recommandations.

Il est intéressant de noter que des commentateurs, tels que Wu *et coll.*[91], ont fait remarquer que l'accent mis sur l'utilisation innovante des renseignements personnels déjà détenus par l'organisation favorisera inévitablement les grandes organisations qui détiennent de grands ensembles de données. Cela peut créer une situation dans laquelle « quelques organisations spéciales, en raison de leurs monopoles de données et de leurs ressources techniques, sont en mesure de décider quels problèmes sont résolus et de quelle manière ». Cependant, avec l'apparition de nouveaux modèles de gouvernance des données qui permettent l'échange de données, « les innovateurs disposant de moins de ressources – y compris les chercheurs individuels, les développeurs citoyens, les communautés locales et les petites et moyennes entreprises – peuvent accéder à suffisamment de données pour alimenter l'IA et l'analyse des données, recadrer les problèmes et les résoudre de manière nouvelle. »[92]

On s'attend également à ce que des modèles de gouvernance novateurs visant à promouvoir un accès plus important, plus équitable et plus rapide aux données gouvernementales par tous les secteurs de l'économie ontarienne voient le jour dans le cadre de la Stratégie pour le numérique et les données du gouvernement[93]. Si les efforts visant à promouvoir un plus vaste échange de données sont certainement louables et doivent continuer à être encouragés, nous recommandons que des modèles de gouvernance appropriés, avec des

mécanismes de surveillance efficaces et indépendants, soient sérieusement envisagés, conçus et mis en œuvre le plus tôt possible, compte tenu de toutes les implications importantes en matière de confidentialité, de sécurité, de justice et d'équité. L'Ontario est dans une position qui lui permet de concevoir un modèle de gouvernance coordonné et intersectoriel qui procurera à la province les avantages prévus des données ouvertes, grâce à la mise en place de protections de la vie privée et de la sécurité.

D. CONCLUSION

De nombreuses mesures importantes n'ont pas été évoquées dans le livre blanc du gouvernement, notamment la notification obligatoire des violations, les dispositions relatives à la définition et à l'application, les dispositions indiquant ce qui se passe en cas de conflit pour les organisations régies par d'autres lois, la conservation des renseignements personnels et les dispositions transitoires. En outre, lorsque des mesures sont évoquées, le libellé détaillé n'est parfois pas fourni. Nous supposons que ces dispositions, ainsi que d'autres dispositions standard et essentielles, figureront dans un éventuel projet de loi, si le gouvernement décide d'aller de l'avant, et nous sommes impatients de nous engager dans une discussion plus détaillée au fur et à mesure que le processus législatif se poursuit.

En fin de compte, nous sommes toujours d'avis que l'Ontario devrait adopter une loi ontarienne sur la protection de la vie privée dans le secteur privé, que la réforme de la *LPRPDE* ait lieu ou non au niveau fédéral. Cela permettra de réagir plus rapidement aux risques toujours croissants auxquels les Ontariens sont confrontés en raison de l'augmentation de leurs activités numériques dans tous les aspects de leur vie. Elle introduira également une approche de la protection de la vie privée fondée sur les droits de l'homme, des protections de la vie privée pour les employés, une attention accrue pour les jeunes et les enfants et la couverture d'un éventail beaucoup plus large d'organisations qui détiennent actuellement des quantités importantes de renseignements personnels sans aucune obligation générale en matière de protection de la vie privée. Cela permettra également au gouvernement d'élaborer une loi axée sur l'Ontario qui tienne compte des besoins des entreprises locales qui luttent pour survivre après la pandémie et qui cherchent des occasions de rivaliser, de croître et de prospérer dans une économie axée sur les données. Qui plus est, cela permettra à l'Ontario de concevoir un modèle de gouvernance des données qui favorise l'innovation respectueuse et viable d'une manière qui protège la vie privée des Ontariens et est digne de leur confiance.

Je vous remercie de me donner l'occasion de répondre aux propositions du gouvernement. Nous espérons que les commentaires susmentionnés contribueront au discours public et aideront le gouvernement à prendre des décisions et à faire des choix. Notre bureau est prêt et engagé à travailler avec le gouvernement pour faire avancer cette importante initiative dans l'intérêt de tous les Ontariens.

ENDNOTES

1 Gouvernement de l'Ontario. « **Modernisation de la protection de la vie privée en Ontario** » (17 juin 2021).

2 Commissaire à l'information et à la protection de la vie privée de l'Ontario, **contribution au document de discussion du gouvernement de l'Ontario, « Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique »** (16 octobre 2020). Consulté le 9 juillet 2021.

3 Gouvernement de l'Ontario, « **Réforme de la protection de la vie privée dans le secteur privé en Ontario : Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique** » (13 août 2020). Consulté le 8 août 2021.

4 Gouvernement de l'Ontario. « **Modernisation de la protection de la vie privée en Ontario** » (17 juin 2021).

5 Voir l'alinéa 26(2)b) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5.

6 Lisa Thompson, ministre des Services gouvernementaux et des Services aux consommateurs, « **Déclaration - Renforcer les mesures de protection de la vie privée pour l'avenir numérique de l'Ontario** » (17 juin 2021). Consulté le 12 juillet 2021.

7 Selon le rapport « Principales statistiques relatives aux petites entreprises 2020 » de Statistique Canada, 86,4 % (4,2 millions) des employés du secteur privé travaillaient pour des petites ou moyennes entreprises (PME).

8 Professeure Teresa Scassa, « **Privacy in the Precision Economy: The Rise of AI-Enabled Workplace Surveillance during the Pandemic** » (8 juin 2021), consulté le 30 juin 2021; Vass Bednar, « **Your boss is watching you while you work** », (18 août 2020), consulté le 30 juin 2021; Darrell M. West, « **How employers use technology to surveil employees** », The Brookings Institute (5 janvier 2021), consulté le 27 août 2021.

9 KPMG Business Outlook Poll, « **Sixty-two per cent of businesses plan to mandate employee vaccines** » (19 août 2021), consulté le 23 août 2021. Voir également : Canadian Lawyer, « **Workplaces showing trend toward mandating COVID vaccinations for employees** » (20 août 2021), consulté le 23 août 2021 et Canadian Lawyer, « **Can employers require new hires to show proof of vaccination?** » (17 mai 2021), consulté le 30 juin 2021.

10 ZDNet, « **One of New York's largest nonprofits suffers data breach** » (31 mai 2019), Insurance Business America, « **Non-profits are a target for data breach** » (16 avril 2019), Charity Village, « **Minimizing the risk of a data breach: a guide for non-profit organizations** » (8 mars 2017), consulté le 12 août 2021.

11 Lawyers Daily, « **Critical privacy, security risks for charities, not-for-profits** », (10 juin 2021), consulté le 10 juillet 2021.

12 CBC News, « **Data theft from Meals on Wheels reveals gap in provincial privacy legislation, expert says** » (11 juillet 2021), consulté le 12 juillet 2021.

13 Personal Information Protection Act, S.B.C. 2003, c. 63

14 Assemblée nationale du Québec, **Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels** (12 juin 2020) art. 81, consulté le 1er 2020.

15 Élections Ontario, « **Asseoir le changement et préparer l'avenir** », rapport annuel 2018-2019.

16 Globe and Mail, « **Liberals face possible federal, provincial privacy probes for use of facial recognition technology » (24 juin 2021)**, consulté le 19 juillet 2021.

17 Les diagrammes sont tirés de l'Enquête sur la consommation de drogues et la santé des élèves de l'Ontario auprès d'élèves de la 7e à la 12e année à moins d'indication contraire. Boak, A., Elton-Marshall, T., Mann, R. E. et Hamilton, H. A. (2020). « **The Mental Health and Well-being of Ontario Students, 1977-2019**: Detailed findings from the Ontario Student Drug Use and Health Survey ». Toronto, Ontario : Centre de toxicomanie et de santé mentale.

18 International Journal of Behavioral Nutrition and Physical Activity, « **Impact of the COVID-19 virus outbreak on movement and play behaviours of Canadian children and youth: a national survey** » (6 juillet 2020), consulté le 12 août 2021.

19 Kathryn Rattigan, « **Smart Toys and How they May be Invading our Privacy** » (15 juillet 2021).

20 Commissaire à l'information et à la protection de la vie privée de l'Ontario, **MC18-48** et **MC17-52**.

21 Ontario Chamber of Commerce, « **Ontario Economic Report 2020** ».

22 Gouvernement de l'Ontario, « **Stratégie ontarienne pour le numérique et les données** » (30 avril 2021), consulté le 12 août 2021.

23 Voir le **Rapport annuel du CIPVP 2021** qui indique, comme dans les années passées, que la vaste majorité des dossiers du secteur public et du secteur de la santé sont réglés par règlement anticipé et au stade de la médiation.

24 Gouvernement de l'Ontario, « **Stratégie ontarienne pour le numérique et les données** » (30 avril 2021), consulté le 12 août 2021.

25 *Loi sur la protection des renseignements personnels et les documents électroniques*, (L.C. 2000, ch. 5), alinéa 26(2)b).

26 Règlement général sur la protection des données de l'Union européenne, article 45 et Commission européenne, **décisions d'adéquation**.

27 Teresa Scassa, « **A Human Rights-Based Approach to Data Protection in Canada** », dans Dubois, E. et Martin-Bariteau, F. (dir.), Citizenship in a Connected Canada: A Research and Policy Agenda, Ottawa (Ontario) : Les Presses de l'Université d'Ottawa (2020).

28 « Nammo c. Transunion of Canada Inc. », 2010 CF 1284, para 74 et 75; « Bertucci c. Banque royale du Canada », 2016 CF 332, para 34.

29 ***Reference re Subsection 18.3(1) of the Federal Courts Act, 2021 FC 723*.**

30 ***Reference re Subsection 18.3(1) of the Federal Courts Act, 2021 FC 723***, para 30, cité par la professeure Teresa Scassa, « **First Step Along the Path to a Right to Be Forgotten in Canada? » (9 juillet 2021), consulté le 12 juillet 2021.**

31 Veuillez consulter, par exemple, le document en anglais seulement de Global Privacy Assembly intitulé **Policy Strategy Working Group 1: Global frameworks and standards** (octobre 2020), consulté le 12 juillet 2021, où il est indiqué que 8 sur 10 cadres généraux de protection de la vie privée font explicitement référence à l'exigence d'indépendance des autorités responsables de la protection de la vie privée.

32 Washington University Law Review, « **Privacy Law's False Promise** » (décembre 2019), consulté le 9 juillet 2021.

33 European Data Protection Board, « **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default** » (novembre 2019).

34 **« R. c. Oakes », [1986] 1 R.C.S. 103; voir également Commissariat à la protection de la vie privée du Canada, « Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle » (novembre 2010), consulté le 23 août 2021**.

35 Paragraphe 4 intitulé Besoins légitimes de la disposition Objectif juste et approprié.

36 ***Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, chap. F.31, para 2(1)**, ***Alberta Personal Information Protection Act*, alinéa1(1)k)**, **Règlement (EU) 2016/679, *Règlement général sur la protection des données***.

37 **« R. c. Spencer », 2014 CSC 43 (CanLII), [2014] 2 R.C.S. 212**

38 **« Banque Royale du Canada c. Trang », 2016 CSC 50, [2016] 2 R.C.S. 412**

39 Commissariat à la protection de la vie privée du Canada, « **Le Commissariat à la protection de la vie privée met à jour les orientations concernant les renseignements sensibles** » (13 août 2021), consulté le 18 août 2021.)

40 Covington « **Five Key Themes from the FTC's Data Portability Workshop** », (30 septembre 2020)

41 U.S. Federal Trade Commission, « **Data To Go: The FTC's Workshop on Data Portability** » (septembre 2020), consulté le 28 juillet 2021 et « **Data To Go: The FTC's Workshop on Data Portability** » [sommaire] (novembre 2020)

42 Future of Privacy Forum, « **FPF Testifies at FTC Data Portability Workshop** », 23 septembre 2020 et Commission européenne, « **Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition -two years of application of the General Data Protection Regulation** », 24 juin 2020.

43 Pour en savoir plus long, voir : Commissaire à l'information et à la protection de la vie privée de l'Ontario, **contribution au document de discussion du gouvernement de l'Ontario, « Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique »** (16 octobre 2020). Consulté le 9 juillet 2021.

44 Assemblée nationale du Québec, ***Projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels***, voir art. 113 du projet de loi créant l'art. 28.1.

45 Commissaire à l'information et à la protection de la vie privée de l'Ontario, « **IPC Comments on the Ontario Government's Consultation on Ontario's *Trustworthy Artificial Intelligence (AI) Framework*** » (juin 2021), consulté le 27 juillet 2021.

46 On entend par système décisionnel automatisé toute technologie qui appuie ou remplace le jugement de décideurs humains au moyen de techniques telles que l'usage de systèmes basés sur des règles, l'analyse de régression, l'analytique prédictive, l'apprentissage automatique, l'apprentissage profond et l'usage de réseaux neuronaux.

47 Gouvernement du Canada, « **Directive sur la prise de décisions automatisée** » (avril 2021), consulté le 27 juillet 2021.

48 Ces techniques comprennent l'analyse de régression qui est une méthode statistique relativement simple et courante.

49 Ben Green et Amba Kak. Slate, « **The False Comfort of Human Oversight as an Antidote to A.I. Harm** » (15 juin 2021), consulté le 27 juillet 2021.

50 Cela comprend la capacité de demander l'accès à des renseignements personnels utilisés pour prendre une décision (et demander qu'elle soit corrigée), de demander les motifs et les facteurs de principe qui ont mené à la décision, la capacité de commenter ou de contester une décision et la capacité de demander l'examen de la décision.

51 Veuillez consulter l'alinéa 2 (Idem) à la page 15 du livre blanc. Veuillez noter que ces éléments sont essentiellement analogues à ceux décrits dans le considérant 71 et à l'alinéa 13(2)f) et au paragraphe 22(3) du Règlement général sur la protection des données (RGPD) de l'Union européenne.

52 Veuillez consulter l'alinéa 3 (Système décisionnel automatisé) à la page 11 du livre blanc.

53 Commissaire à l'information et à la protection de la vie privée de l'Ontario, **contribution au document de discussion du gouvernement de l'Ontario, « Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique »**, p. 11 (16 octobre 2020). Consulté le 10 juillet 2021.

54 Cela a été confirmé dans le jugement de la Cour suprême du Canada « **Banque Royale du Canada c. Trang », 2016 CSC 50, [2016] 2 R.C.S. 412**.

55 Règlement général sur la protection des données de l'Union européenne, articles 24, 28 et 29.

56 **« R. c. Spencer », 2014 CSC 43, [2014] 2 RCS 212** et **« R. c. Orlandis-Habsburgo », 2017 ONCA 649**.

57 « **Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta** » (2 février 2021), consulté le 13 juillet 2021.

58 Les chercheurs étudient depuis un certain temps le concept de représentation visuelle des renseignements personnels. Le premier effort le mieux connu est sans doute le concept de l'étiquetage sur la protection de la vie privée semblable à l'étiquetage nutritionnel mis au point en 2009 par une équipe de l'Université Carnegie Mellon (**http://cups.cs.cmu.edu/privacyLabel/**). Plus récemment, nous avons constaté des efforts tels que l'étiquetage sur la protection de la vie privée et la sécurité de l'IdO [Internet des objets] (**https://iotsecurityprivacy.org/**) et la fiabilité numérique pour l'iconographie des places et des habitudes (**https://dtpr.helpfulplaces.com/**), et en décembre 2020, Apple a lancé les étiquettes sur la protection de la vie privée pour les applications dans son App Store (**https://developer.apple.com/app-store/app-privacy-details/**). Dans chaque cas, l'intention est de fournir aux particuliers les renseignements nécessaires dans un langage facile à comprendre.

Même si aucun de ces efforts (hormis les étiquettes d'Apple) n'a atteint un niveau élevé d'adhésion, cette approche est prometteuse en tant que premier mécanisme de transparence pour donner une compréhension rapide des pratiques d'une organisation.

59 Par exemple, le nombre de demandes reçues, le nombre de demandes aboutissant à une divulgation, le nombre de divulgations demandées (p. ex., à la suite d'une ordonnance judiciaire), le nombre de personnes dont les renseignements ont été divulgués, etc.

60 Assemblée mondiale pour la protection de la vie privée. **Résolution sur la transparence** (27 octobre 2015), consulté le 27 juillet 2021.

61 Commissaire à l'information et à la protection de la vie privée de l'Ontario. « **Divulgation de renseignements personnels à un organisme d'application de la loi** » (novembre 2018).

62 Gouvernement du Canada. « ***Lignes directrices concernant la production de rapports sur les mesures de transparence*** » (juin 2015), consulté le 23 août 2021.

63 Article 35.1 : « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. »

Alinéa 35.3(a) : « L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise pour l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

64 L'« organisation qui transfère les données » et le « fournisseur de services » correspondent à l'« autorité de contrôle » et au « responsable du traitement » qui sont mentionnés dans le RGPD. La section 4 du RGPD établit la relation entre l'autorité de contrôle et le responsable du traitement, dont les obligations de l'autorité de contrôle (article 24) et du responsable du traitement (article 28).

65 Par exemple, dans le projet de loi C-11, cela se trouve au paragraphe 7(2) : Les renseignements personnels relèvent de l'organisation qui décide de les recueillir et établit les fins pour lesquelles ils sont recueillis, utilisés ou communiqués, qu'elle les recueille, utilise ou communique elle-même ou qu'un fournisseur de services le fasse pour elle.

66 Nous notons que Google a récemment fait un premier pas dans ce sens en annonçant son intention d'adopter une politique permettant aux personnes de moins de 18 ans (ou à leurs parents ou tuteurs) de demander la désindexation de leurs images. Veuillez consulter Google, « **Giving kids and teens a safer experience online** » (10 août 2021), consulté le 16 août 2021.

67 **Selon l'article 123 de la Data Protection Act 2018**, le commissaire doit préparer un code de pratique qui contient des orientations qu'il juge opportunes sur les normes de conception adaptées à l'âge de services sociétaux d'information que des enfants sont susceptibles de consulter. En vertu de l'article 125(1), lorsqu'un code a été préparé en vertu de l'article 123... a) le commissaire doit en présenter la version finale au secrétaire d'État et b) le secrétaire d'État doit déposer le code devant le parlement.

68 Bureau du commissaire à l'information du Royaume-Uni, « **Age appropriate design: a code of practice for online services** » (2 septembre 2020), consulté le 16 août 2021.

69 *Règlement général sur la protection des données* de l'Union européenne, article 41(1).

70 Projet de loi C-11, par. 76(3) et 77(1).

71 Bureau du commissaire à l'information du Royaume-Uni, « **Sandbox beta phase discussion paper** » (30 janvier 2019), consulté le 27 juillet 2021.

72 Autorité norvégienne de protection des données, « **Sandbox for responsible artificial intelligence** », consulté le 27 juillet 2021.

73 Commission de l'énergie de l'Ontario, « **L'espace innovation CEO** », consulté le 27 juillet 2021.

74 Commissaire à l'information et à la protection de la vie privée de l'Ontario, « **Documents d'orientation** ».

75 Projet de loi C-11, al. 109e).

76 Commissaire à l'information et à la protection de la vie privée de l'Ontario, **contribution au document de discussion du gouvernement de l'Ontario, « Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique »** (16 octobre 2020), consulté le 10 juillet 2021.

77 *LPRPS* art. 62 et *Loi sur les services à l'enfance, à la jeunesse et à la famille* (*LSEJF*), 2017, L.O. 2017, ch. 14, ann. 1, art. 322 [*LSEJF*].

78 Le projet de dispositions manque d'uniformité à cet égard. Le paragraphe (1) des dispositions proposées en matière de sanctions administratives pécuniaires ne fait pas référence à des infractions au Règlement en vertu de la Loi. D'autres projets de dispositions, quant à eux, font référence à la « Loi » et à « son Règlement ».

79 Voir la *LPRPS*, al. 72(1)a). Une infraction similaire est incluse dans la Personal Information Protection Act de l'Alberta, SA 2003, ch. P-6.5, al. 59(1)a).

80 Voir la *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, ch. F.31, al. 61(1)e) [*LAIPVP*]; la *Loi sur l'accès à l'information municipale et la protection de la vie privée*, L.R.O. 1990, ch. M.56, al. 48(1)e) [*LAIMPVP*]; et la *LPRPS*, al. 72(1)h).

81 Voir la *LAIPVP*, al. 61(1)c); la *LAIMPVP*, al. 48(1)c); et la *LPRPS*, al. 72(1)b).

82 Voir la *LAIPVP*, al. 61(1)c.1); et la *LAIMPVP*, al. 48(1)c.1). Une infraction similaire est incluse dans la *LPRPS*, al. 71(1)d).

83 Cette infraction devrait être incluse, si elle n'est pas déjà couverte par l'infraction de dénonciation dont il est question dans le livre blanc. Pour des infractions semblables, voir la

LPRPS, par. 70 et al. 72(1)J); projet de loi C-11, par. 124(1) et art. 125; et la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, par. 27.1(1) et art. 28.

84 Voir la *LAIPVP*, art. 61; la *LAIMPVP*, art. 48; et *la LPRPS*, art. 72; et la *LSEJF*.

85 Similaire à l'art. 65 de la *LPRPS*.

86 Notre définition proposée est semblable à, et compatible avec, celle qui figure dans la *Loi sur la protection des renseignements personnels sur la santé de l'Ontario*.

87 Voir, par exemple, le *Règlement général sur la protection des données de l'Union européenne*, considérant 26 : « Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. »

88 Voir, par exemple, Rocher et coll., « **Estimating the success of re-identifications in incomplete datasets using generative models** », Nature Communications, vol. 10, art. no 3069 (23 juillet 2019), consulté le 16 août 2021.

89 Voir, par exemple, l'étude de cas no 6 (Case Study #6) du rapport de mars 2021 du Canadian Anonymization Network, « **Practices for Generating Non-Identifiable Data** », consulté le 27 juillet 2021.

90 Voir, par exemple, El Emam, Mosquera et Bass : « **Evaluating Identity Disclosure Risk in Fully Synthetic Health Data** », Journal of Medical Internet Research, vol. 22, no 11, 2020.

91 Wu et coll. Data & Policy, « **How data governance technologies can democratize data sharing for community well-being** » (juillet 2021), consulté le 27 juillet 2021.

92 *Ibid*.

93 Gouvernement de l'Ontario, « **Créer un Ontario numérique** » (30 avril 2021); gouvernement de l'Ontario, « **L'Ontario nomme un conseiller spécial pour l'établissement d'un office des données** » (6 août 2021), consulté le 16 août 2021.

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2, rue Bloor Est,
bureau 1400
Toronto (Ontario)
Canada M4W 1A8
Telephone: 416-326-3333

www.ipc.on.ca
info@ipc.on.ca

Septembre 2021