Modernisation de la protection de la vie privée en Ontario

Autonomiser les Ontariens et favoriser l'économie numérique

LIVRE BLANC

Attention :

Les dispositions incluses dans ce livre blanc ont pour but de faciliter le dialogue concernant son contenu. Il est à noter qu'il n'aura pas force de loi à moins qu'un projet de loi ne soit adopté par l'Assemblée législative de l'Ontario. Si la décision est prise de présenter un projet de loi à l'Assemblée législative, les commentaires reçus lors de la consultation seront pris en compte lors de la préparation du projet de loi. Le contenu, la structure, la forme et le libellé des deux versions linguistiques de l'ébauche de consultation sont susceptibles d'être modifiés à la suite du processus de consultation et à la suite de l'examen, de la révision et de la correction par le Bureau des conseillers législatifs.

1 Introduction

La vision du gouvernement de l'Ontario est de faire de l'Ontario le territoire numérique le plus avancé au monde. Comme l'indique la Stratégie pour le numérique et les données récemment annoncée par le gouvernement, cet objectif permet aux Ontariens d'acquérir les compétences, les droits et les possibilités nécessaires pour participer pleinement au monde numérique, y travailler et s'y épanouir. Les entreprises bénéficieront de nouveaux investissements dans l'infrastructure à large bande et de données publiques, tandis que les gens bénéficieront d'un accès accru à des services gouvernementaux en ligne fiables et conviviaux.

La protection de la vie privée numérique est un élément essentiel de ce travail. Il s'agit de veiller à ce que les Ontariens aient le pouvoir de contrôler les données personnelles qu'ils partagent, quand ils les partagent et avec qui ils les partagent. Il s'agit d'une priorité essentielle du gouvernement de l'Ontario. Surtout avec la pandémie de COVID-19 qui oblige des millions d'Ontariens à vivre leur vie presque entièrement en ligne, il est essentiel pour l'avenir de notre économie et le bien-être de notre population de mettre à jour nos lois sur la protection de la vie privée.

En Ontario, la vie privée dans le secteur privé est régie par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du gouvernement fédéral. L'année dernière, le gouvernement du Canada a présenté le projet de loi C-11, *Loi de 2020 sur la mise en œuvre de la Charte du numérique,* pour remplacer la LPRPDE et moderniser le régime fédéral de protection de la vie privée. Bien qu'elle comporte quelques nouveautés bienvenues, la loi proposée présente plusieurs points faibles : son cadre de consentement pourrait permettre aux organisations de collecter et d'utiliser les données des citoyens à des fins commerciales à leur insu; elle ne prévoit pas de protections spéciales pour les enfants et les jeunes; et ses droits numériques ne vont pas assez loin pour protéger les personnes contre les nouveaux risques comme la surveillance.

Le gouvernement de l'Ontario s'est engagé à combler ces lacunes. Après avoir soigneusement examiné les commentaires reçus lors de notre consultation sur la réforme de la protection de la vie privée de 2020[1] , et les commentaires des experts en protection de la vie privée sur le projet de loi C-11, l'Ontario envisage des propositions qui mettraient en œuvre un droit fondamental à la vie privée pour les Ontariens, introduiraient davantage de garanties en ce qui a trait aux technologies d'intelligence artificielle (IA), introduiraient des protections dédiées pour les enfants, mettraient à jour les règles de consentement pour refléter l'économie moderne des données, encourageraient l'innovation responsable et corrigeraient les déséquilibres de pouvoir systémiques qui ont émergé entre les personnes et les organisations qui recueillent et utilisent leurs données.

Dans ses observations approfondies, Patricia Kosseim, commissaire à l'information et à la protection de la vie privée de l'Ontario, félicite le gouvernement d'avoir entamé un dialogue sur ces questions importantes. Elle souligne la nécessité d'adopter un régime de réglementation et de protection de la vie privée fondé sur des principes, équitable et bien équilibré, pragmatique, souple et proportionné, soulignant que « les consommateurs, les entreprises et les gouvernements ont tous compris que la protection de la vie privée, loin d'empêcher de trouver des solutions innovantes, est essentielle à leur réussite ».

Ce livre blanc présente les propositions de l'Ontario et fournit des exemples de langage législatif qui démontrent comment ces protections pourraient être reflétées dans la loi. Ces propositions sont conformes à la Stratégie numérique et des données du gouvernement et s'appuient sur les efforts récents visant à améliorer la protection de la

[1] Nous avons reçu un large éventail de réactions et de participations à la consultation : 175 organisations consultées, 14 tables rondes sectorielles, 97 soumissions écrites, 20 entretiens avec des spécialistes universitaires et juridiques de la protection de la vie privée, 929 réponses à l'enquête en ligne et 2 assemblées publiques virtuelles.

vie privée dans le domaine de la santé dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS). Si elles sont adoptées, ces propositions s'harmoniseront avec les autres lois ontariennes sur la protection de la vie privée et réduiront au minimum le fardeau réglementaire des organisations ontariennes.

En bref, les propositions présentées dans ce document sont organisées selon les thèmes suivants :

- Une approche de la vie privée fondée sur les droits
- L'utilisation sûre de la prise de décision automatisée
- Améliorer le consentement et les autres utilisations licites des renseignements personnels
- Transparence des données pour les Ontariens
- Protéger les enfants et les jeunes
- Un régime réglementaire équitable, proportionné et favorable
- Soutenir les innovateurs de l'Ontario

Ces propositions n'auront de sens que si leurs protections sont complètes. La portée du régime fédéral de protection de la vie privée est limitée aux activités commerciales. Cela signifie que de nombreuses organisations du secteur privé, y compris les organismes de bienfaisance, les syndicats, les associations et autres organismes sans but lucratif, ne sont pas couvertes par le projet de loi proposé, malgré la collecte et l'utilisation des renseignements personnels des Ontariens par ces organisations. Pour combler cette lacune, la province envisage d'élargir la portée des exigences en matière de protection de la vie privée sous chacun de ces thèmes afin d'inclure les organisations non commerciales, garantissant ainsi que les renseignements personnels des Ontariens bénéficient d'une couverture et d'une protection adéquates dans tous les aspects de la vie.

Au cours de l'élaboration de ce livre blanc, le Commissariat à la protection de la vie privée du Canada (CPVP) a, de façon indépendante, présenté au gouvernement fédéral des commentaires réfléchis sur le projet de loi C-11 par le biais d'une soumission publique. Bien que ce mémoire ne traite pas directement des propositions de l'Ontario en matière de protection de la vie privée, nous vous encourageons à tenir compte du rapport et des recommandations du CPVP lorsque vous répondrez à ce livre blanc. Veuillez consulter les observations publiques réfléchies de la commissaire à l'information et à la protection de la vie privée de l'Ontario concernant les propositions de l'Ontario relatives à la protection de la vie privée.

2 Principaux domaines de réforme

Une approche de la vie privée fondée sur les droits

Problème :

Compte tenu des progrès rapides de la technologie qui élargissent considérablement la capacité des organisations à recueillir, à utiliser et à échanger des renseignements personnels, de nouvelles règles et de nouveaux droits sont nécessaires pour protéger les Ontariens contre des pratiques potentiellement déloyales et pour maintenir un niveau élevé de confiance dans l'économie numérique.

Objectif :

Conformément aux recommandations du Commissaire à la protection de la vie privée du Canada, l'Ontario pourrait établir un droit fondamental à la vie privée comme principe sous-jacent à une loi provinciale sur la protection de la vie privée, garantissant ainsi la protection des Ontariens, indépendamment des intérêts commerciaux.

*

Lors de la consultation provinciale de 2020 sur la réforme de la protection de la vie privée, les Ontariens ont exprimé un niveau raisonnable d'inquiétude quant au fait que leurs données ne sont pas protégées lorsque la vie privée entre en concurrence avec les intérêts des organisations. Cette inquiétude a entraîné une méfiance et une incertitude quant aux pratiques en matière de données dans toute la province. La protection de la vie privée n'est pas une préoccupation purement individuelle; elle fait plutôt partie du capital social d'une société démocratique, en corrélation avec les libertés de parole, d'expression et d'association. De nombreux experts ont fait valoir que la valeur de la vie privée est donc mieux exprimée comme un droit fondamental, plutôt que comme un équilibre entre des intérêts concurrents.

La protection de la vie privée est reconnue par *la Déclaration universelle des droits de l'homme*, et le *Règlement général sur la protection des données* (RGPD) de l'Europe est fondé sur un cadre de droits individuels en matière de données. Cependant, le système fédéral se limite aux activités commerciales et les lois canadiennes n'ont généralement pas adopté une approche ouvertement fondée sur les droits. Le Québec fait exception, car sa loi sur la protection de la vie privée dans le secteur privé reconnaît et met en œuvre le droit à la vie privée explicitement énoncé dans la *Charte des droits et libertés de la personne* et le *Code civil* du Québec.

L’Ontario envisage de reconnaître un droit fondamental à la vie privée en Ontario. Cette approche pourrait prendre la forme d’un préambule qui exposerait ce droit fondamental de la manière suivante :

> **Préambule**
>
> La vie privée est une valeur fondamentale de la société. Tout particulier a un droit fondamental au respect de sa vie privée et à la protection de ses renseignements personnels.
>
> L’évolution de la technologie a permis aux organisations de recueillir facilement de grandes quantités de renseignements personnels sur les particuliers, ce qui a souvent pour effet de réduire le contrôle qu’un particulier exerce sur ses renseignements personnels.
>
> Pour inspirer la confiance des particuliers, les organisations doivent être soumises à des règles guidées par les principes de proportionnalité, d’équité et d’adéquation en ce qui a trait à la collecte, à l’utilisation ou à la divulgation des renseignements personnels.

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. Ces caractéristiques seront décrites dans les prochaines sections. Il faudra aussi une définition claire des renseignements personnels qui tienne compte des formes très variables sous lesquelles les données sont trouvées et utilisées. Dans le contexte actuel, les organisations utilisent souvent des renseignements qui ont été dépersonnalisés par rapport à leur état initial (voir Soutien aux innovateurs de l’Ontario), ou des renseignements qui ont été dérivés ou déduits de renseignements personnels par un raisonnement probatoire ou d’autres processus analytiques. Bien qu’il puisse être utile de conserver une définition des renseignements personnels qui soit simple, claire et distincte de ces dérivations, un régime moderne de protection de la vie privée doit néanmoins décider comment traiter les données qui apparaissent sous différentes formes. Nous invitons les Ontariens à nous faire part de leurs commentaires sur la meilleure façon d’atteindre cet équilibre si ces termes étaient envisagés dans une prochaine loi sur la protection de la vie privée.

Objectif juste et approprié

Les lois modernes sur la protection de la vie privée protègent notamment les personnes en exigeant que les organisations ne recueillent, n’utilisent et ne divulguent les renseignements personnels des personnes qu’à des fins objectivement justes et appropriées dans les circonstances. Le concept de « juste et approprié » est une protection globale qui définit les paramètres des activités autorisées. Il prévoit que les renseignements ne peuvent être collectés, utilisés et divulgués qu’à des fins auxquelles

une personne s'attendrait raisonnablement, quels que soient les motifs légaux de collecte, d'utilisation et de divulgation des renseignements personnels qui peuvent s'appliquer. Cela signifie qu'une organisation devra satisfaire à ce critère, qu'elle ait obtenu le consentement de la personne concernée ou qu'elle s'appuie sur une autre autorité légale. L'Ontario envisage d'énoncer ces dispositions de la manière suivante, afin d'avoir une limitation similaire pour la collecte, l'utilisation ou la divulgation de renseignements personnels, comme dans le projet de loi fédéral C-11 et d'autres lois canadiennes existantes sur la protection de la vie privée :

Fins acceptables
(1) L'organisation ne peut recueillir, utiliser ou divulguer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait équitables et appropriées dans les circonstances.

Facteurs à prendre en compte
(2) Les facteurs suivants doivent être pris en compte pour établir le caractère équitable et approprié des fins visées au paragraphe (1) :

1. Le volume, la nature et le caractère délicat des renseignements personnels, notamment la question de savoir si l'organisation a pris des mesures pour les dépersonnaliser.
2. La question de savoir si la collecte, l'utilisation ou la divulgation est nécessaire pour répondre aux besoins légitimes de l'organisation.
3. L'existence ou non de moyens portant une atteinte moindre à la vie privée du particulier et permettant d'atteindre les fins visées à un coût et avec des avantages comparables.
4. La proportionnalité entre l'atteinte à la vie privée du particulier et les avantages pour l'organisation, au regard des moyens, techniques ou autres, mis en place par l'organisation afin d'atténuer les effets de l'atteinte pour le particulier.

Établissement des fins
(3) L'organisation établit et consigne les fins auxquelles les renseignements personnels sont recueillis, utilisés ou divulgués avant la collecte ou au plus tard au moment de celle-ci.

Besoins légitimes
(4) Pour l'application de la disposition 2 du paragraphe (2), les besoins légitimes d'une organisation ne comprennent pas, selon le cas :

a) la surveillance ou le profilage des particuliers âgés de moins de 16 ans dans le but d'influencer leur comportement ou leurs décisions;

b) les fins dont on sait qu'elles causent, ou qui sont susceptibles de causer, un préjudice grave aux particuliers ou à des groupes de particuliers;
c) les fins qui contreviendraient à une loi de l'Ontario ou du Canada;
d) les autres fins prescrites.

Pour compléter le concept de fins justes et appropriées, l'Ontario envisage également d'imposer aux organisations l'obligation générale de limiter leur collecte, leur utilisation et leur communication aux seuls renseignements personnels nécessaires à la réalisation des fins prévues. Cette disposition de limitation appuie le principe de minimisation des données « moins, c'est plus », ce qui pourrait contribuer à établir un cadre cohérent et légal qui consacre le droit à la vie privée des Ontariens.

RESTRICTIONS APPLICABLES À LA COLLECTE, À L'UTILISATION ET À LA DIVULGATION

Restrictions applicables à la collecte, à l'utilisation et à la divulgation
L'organisation ne peut recueillir, utiliser ou divulguer des renseignements personnels que si les conditions suivantes sont réunies :

a) les renseignements personnels sont nécessaires aux fins qu'elle a établies et consignées en application du [paragraphe];
b) elle obtient le consentement du particulier à l'égard de la collecte, de l'utilisation ou de la divulgation, ou elle est par ailleurs autorisée à recueillir, utiliser ou divulguer, selon le cas.

Bien que le projet de loi C-11 exige que la collecte, l'utilisation ou la communication de renseignements personnels soit « appropriée dans les circonstances », l'exigence d'équité pourrait renforcer cette composante fondamentale du cadre de protection de la vie privée de l'Ontario. La commissaire à l'information et à la protection de la vie privée de l'Ontario a souligné que le principe de l'équité (entre autres) brille par son absence dans la LPRPDE, et qu'il devrait être intégré dans toute loi moderne de protection de la vie privée. L'inclusion du terme « équité » aurait pour but de renforcer une interprétation de la loi davantage axée sur les citoyens et d'intégrer ces objectifs aux principes fondés sur les droits énoncés dans le préambule. Pour améliorer cet aspect de la loi par rapport au projet de loi C-11, l'Ontario pourrait exiger des organisations qu'elles tiennent compte du volume et de la nature des renseignements en plus de leur « sensibilité ». Pour donner plus de sens à cette dernière, l'Ontario pourrait également envisager, à l'instar du GDPR de l'Europe et du projet de loi 64 du Québec, de fournir une définition des renseignements sensibles qui éclairerait l'application de ces principes. Cette définition pourrait être fondée sur le risque, ou sur des classes ou des catégories d'informations spécifiques. De nombreux experts en matière de protection de la vie privée ont recommandé une définition combinant les deux approches.

L’obligation d’avoir un « objectif juste et approprié » pourrait également être formulée de manière à tenir compte d’autres facteurs pertinents. Par exemple, elle pourrait également exiger des organisations qu’elles se demandent si elles ont pris des mesures pour dépersonnaliser les renseignements. De manière significative, l’Ontario pourrait également clarifier le concept de « besoin légitime » de renseignements personnels en introduisant des limitations spécifiques, telles que l’interdiction des fins qui pourraient causer un préjudice à des personnes ou à des groupes ou contrevenir à d’autres lois provinciales ou fédérales. (L’interdiction éventuelle liée à la surveillance et au profilage des personnes de moins de 16 ans, visée par l’une des dispositions ci-dessus, sera présentée dans une prochaine section).

Les dispositions proposées décrites ci-dessus témoignent d’une approche axée sur la protection de la vie privée qui établit des droits clairs en la matière pour les personnes et limite les organisations à la collecte, à l’utilisation et à la communication de renseignements personnels uniquement à des fins légitimes qu’une personne raisonnable trouverait justes et appropriées dans les circonstances. En limitant la collecte, l’utilisation ou la communication de renseignements personnels à des fins objectivement « justes et appropriées », ces dispositions proposées établiraient des limites fondées sur des principes que les organisations doivent respecter - et devraient respecter - si elles veulent recueillir, utiliser et communiquer les renseignements personnels des Ontariens. Ces limites pourraient, conformément à d’autres lois modernes sur la protection de la vie privée, précéder tous les autres pouvoirs énoncés dans la loi et, par conséquent, jouer un rôle essentiel dans le maintien du droit fondamental des Ontariens à la vie privée.

Droits de mobilité, d’élimination, d’accès et de rectification des données

Le droit global à la vie privée est soutenu par l’affirmation d’importants droits relatifs aux données qui permettent aux Ontariens d’accéder à leurs renseignements personnels, de les corriger, de les transférer et de les éliminer. Le droit d’accès à ses renseignements personnels et le droit de demander leur correction se trouvent dans les lois modernes sur la protection de la vie privée, notamment la LPRPDE, les lois sur la protection de la vie privée de l’Alberta et de la Colombie-Britannique, et la loi existante du Québec. Le droit des individus d’obtenir et de transférer leurs renseignements personnels, connu sous le nom de « mobilité des données » ou « portabilité des données », se trouve maintenant dans le RGPD européen, le projet de loi C-11 du Canada et le projet de loi 64 du Québec. Tous ces droits sont désormais considérés comme des caractéristiques essentielles des régimes modernes de protection de la vie privée.

Un autre droit que l’on retrouve dans les lois plus récentes est le droit pour les personnes d’exiger des organisations, sous réserve de certaines restrictions, qu’elles éliminent leurs renseignements personnels. L’Ontario envisage également un droit

d'élimination, également connu dans certains territoires sous le nom de droit à l'effacement ou à la suppression, dans ce sens :

> **Élimination à la demande du particulier**
> (1) L'organisation qui reçoit d'un particulier une demande écrite d'élimination des renseignements personnels qu'elle a recueillis auprès de lui procède dès que possible à leur élimination sauf si, selon le cas :
>
> a) l'élimination entraînerait celle des renseignements personnels concernant un autre particulier et ces renseignements ne peuvent être séparés;
> b) d'autres exigences de la présente loi, d'une autre loi ou d'une loi ou d'un règlement de l'Ontario ou du Canada, ou des dispositions raisonnables d'un contrat empêchent l'organisation d'éliminer les renseignements;
> c) les renseignements personnels ont été divulgués dans le cadre d'une instance judiciaire ou sont par ailleurs mis à la disposition d'une partie à une instance;
> d) d'autres circonstances prescrites existent.

L'Ontario accueille favorablement les commentaires du public afin de déterminer la portée et les limites appropriées de ce droit. Par exemple, le commissaire à la protection de la vie privée du Canada a recommandé que le droit à l'effacement englobe tous les renseignements qu'une organisation détient sur une personne, y compris ceux provenant de tiers comme les courtiers en données, plutôt que de se limiter aux renseignements recueillis directement auprès d'elle. La commissaire à l'information et à la protection de la vie privée de l'Ontario a également recommandé que les personnes mineures fassent l'objet d'une attention particulière en ce qui concerne le droit à l'effacement, car les jeunes devraient avoir la liberté d'expérimenter et de se découvrir sans s'inquiéter de la permanence des renseignements qu'ils affichent sur eux-mêmes en ligne. Dans le cadre de ce droit à l'effacement, l'Ontario pourrait également envisager d'exiger des organisations qu'elles fournissent des raisons à la personne dans les cas où une demande est refusée, et qu'elles informent la personne des recours disponibles. Les exigences en matière de retrait s'appliqueraient également à tous les fournisseurs de services qui pourraient avoir reçu les renseignements pour les aider à atteindre les objectifs de la collecte initiale.

> **Élimination par le fournisseur de services**
> L'organisation qui a transféré des renseignements personnels à un fournisseur de services et qui procède par la suite à leur élimination fait ce qui suit dès que possible :
>
> a) si elle a reçu une demande d'un particulier, elle en informe le fournisseur de services;
> b) elle veille à ce que le fournisseur de services procède à l'élimination des renseignements;

c) elle obtient la confirmation du fournisseur de services que les renseignements ont été éliminés.

Outre le droit de la personne de demander la destruction des renseignements personnels qu'elle a elle-même fournis, l'Ontario pourrait également envisager la possibilité d'aller au-delà du droit fédéral d'élimination, en inscrivant l'obligation pour les organisations de désindexer les résultats de recherche contenant des renseignements personnels sur une personne qui ont été affichés par d'autres. Ce « droit à l'oubli », s'il est introduit, serait soumis à des préoccupations et à des considérations compensatoires en matière de liberté d'expression, comme la disposition équivalente incluse dans le projet de loi 64 du Québec (article 28.1).

En ce qui concerne la portabilité des données, l'Ontario envisage une proposition qui permettrait aux personnes de demander à une organisation une copie lisible par machine de leurs données, ce qui leur permettrait de transférer leurs activités à un autre fournisseur. Ce droit devrait notamment s'appuyer sur des normes sectorielles qui permettraient d'établir des exigences et des attentes techniques cohérentes pour les organisations qui répondraient à ces demandes. Par exemple, le commissaire à la protection de la vie privée du Canada a recommandé, en référence au projet de loi C-11, que les droits à la mobilité des données s'étendent aux « renseignements inférés » (décrits ci-dessus). L'Ontario souhaite recevoir des avis sur ces questions de portée et sur la meilleure façon de clarifier les limites appropriées de ce droit afin de s'assurer qu'il atteint l'objectif visé sans devenir impraticable pour les organisations qui le mettraient en œuvre.

Si ce droit est accordé, l'Ontario élaborerait ces normes en concertation avec différents secteurs de la province, conformément aux recommandations qu'a formulées la commissaire à l'information et à la protection de la vie privée lors de la consultation de 2020 sur la réforme de la protection de la vie privée. En accordant ce droit aux particuliers, on pourrait accroître la concurrence entre les fournisseurs de services et l'innovation de ces derniers. Un droit à la portabilité des données pourrait être rendu possible par des dispositions comme celle-ci :

Divulgation conformément à un cadre de mobilité des données
(1) Sous réserve des règlements et sur demande écrite du particulier, l'organisation divulgue, dès que possible, les renseignements personnels qu'elle a recueillis auprès de lui à l'organisation que ce dernier désigne si ces deux organisations sont soumises à un cadre de mobilité des données prévu par règlement.

Communication exigée : élimination
(2) L'organisation qui reçoit d'un particulier une demande visée au paragraphe (1) informe celui-ci qu'il peut demander que l'organisation élimine ses renseignements personnels.

Enfin, l'Ontario envisage de donner aux personnes un droit d'accès et de correction de leurs renseignements personnels qui sont sous la garde d'une organisation. Ce droit est similaire à celui que l'on trouve dans d'autres lois canadiennes et internationales sur la protection de la vie privée, ainsi qu'aux droits d'accès et de correction actuellement prévus par la *Loi sur l'accès à l'information et la protection de la vie privée.*

Renseignements et accès
(1) Sur demande d'un particulier, l'organisation lui indique si elle détient des renseignements personnels qui le concernent et l'informe sur leur utilisation et leur divulgation. Elle lui donne aussi accès aux renseignements.

Nom des tiers ou catégories de tiers
(2) Si l'organisation a divulgué les renseignements, elle fournit au particulier le nom des tiers ou les catégories de tiers auxquels ils ont été divulgués, et ce, même lorsqu'elle les a divulgués sans son consentement.

Système décisionnel automatisé
(3) Si l'organisation a utilisé un système décisionnel automatisé pour faire une prédiction, formuler une recommandation ou prendre une décision concernant le particulier, elle lui fournit, à sa demande, une explication de la prédiction, de la recommandation ou de la décision et lui indique la provenance des renseignements personnels utilisés pour faire la prédiction, formuler la recommandation ou prendre la décision.

Le droit d'accès serait un outil important permettant aux Ontariens de suivre l'utilisation de leurs données et de s'assurer de leur exactitude entre les organisations et les plates-formes. (L'exigence de transparence proposée pour la prise de décision automatisée sera décrite plus en détail dans la section suivante).

Questions de discussion :

- Le préambule proposé dans cette section inclut-il les bons principes, raisons et valeurs pour guider l'interprétation d'un éventuel projet de loi sur la protection de la vie privée ?
- Comment les concepts de renseignements personnels et de renseignements personnels « sensibles » doivent-ils être définis dans la loi ?

- Les « objectifs justes et appropriés » proposés dans ce document fournissent-ils des normes de responsabilité adéquates et claires pour les organisations et les prestataires de services ?
- Quelle doit être la portée des droits à l'effacement et à la mobilité des données ? Devraient-ils inclure toutes les informations qu'une organisation possède sur une personne, ou seulement les informations fournies par cette dernière ?

L'utilisation sûre de la prise de décision automatisée

Problème :

Il est clair que les technologies d'IA, telles que les systèmes de décision automatisés, offrent des avantages considérables pour les organisations et l'économie. Cependant, de nouveaux risques tels que la surveillance et le biais algorithmique sont apparus et nécessitent une plus grande responsabilisation. Le projet de loi C-11 améliore les droits des Ontariens en matière de transparence algorithmique, mais il n'inclut pas les protections dont bénéficient les citoyens d'autres juridictions.

Objectif :

En s'appuyant sur les consultations publiques menées par le gouvernement pour créer un cadre de confiance pour l'IA, l'Ontario pourrait interdire l'utilisation de systèmes automatisés de prise de décision en matière d'IA lorsqu'ils risquent de causer un préjudice aux citoyens, prévoir des droits renforcés pour informer les Ontariens du moment et de la manière dont leurs données sont utilisées par ces technologies, et leur donner le droit de s'opposer à ces utilisations, ou du moins de les contester.

*

L'intelligence artificielle a révolutionné le paysage moderne des données. De nombreux secteurs en Ontario ont adopté des technologies d'apprentissage automatique pour aider ou remplacer l'analyse et la prise de décision humaines. Bien que ces technologies offrent de précieuses innovations, elles ont également augmenté les capacités de surveillance de la société moderne et, par conséquent, accru les risques associés aux droits individuels. L'intelligence artificielle permet aux organisations de relier des données provenant de différentes sources afin d'analyser et de prédire des schémas d'activité complexes, de déduire des informations très sensibles sur les personnes, de surveiller leurs mouvements et leurs comportements, et d'influencer leurs actions - parfois à l'insu de l'intéressé ou sans qu'il puisse les contrôler. Bien que la surveillance ne nécessite pas toujours l'IA, et que tous les processus d'IA ne constituent pas de la surveillance, l'intersection de ces pratiques peut poser un risque indu pour les citoyens. Ces capacités évoluées de surveillance peuvent compromettre les droits et la liberté des

Ontariens et créer un important déséquilibre de pouvoir entre les individus et les organisations qui utilisent leurs données.

Profilage et prise de décision automatisée

Les législateurs de nombreux territoires, dont l'Europe et le Québec, réagissent à l'IA en donnant aux individus le droit d'être informés de son utilisation, de la commenter, de s'y opposer ou de la contester. Ces droits liés à l'IA reconnaissent les implications de l'IA pour le droit fondamental à la vie privée et d'autres droits. Si l'IA peut, là encore, présenter des avantages, l'Ontario pourrait offrir des droits similaires aux individus. La présente section décrit les exigences proposées en ce qui concerne le profilage et la prise de décision automatisée.

Le terme « profilage « désigne généralement la pratique consistant à utiliser des renseignements personnels pour créer des descriptions représentatives des caractéristiques, activités ou attributs d'une personne. L'Ontario envisage la définition suivante du profilage :

> « profilage » : toute forme de collecte, d'utilisation ou de divulgation automatisée de renseignements personnels dans le but d'évaluer, d'analyser ou de prédire certains aspects concernant un particulier.

Bien que le profilage soit une pratique ancienne, les progrès de l'IA permettent désormais aux organisations de puiser dans diverses sources pour créer des ensembles de données plus complets. Les profils sont devenus essentiels à l'administration de nombreux types d'activités commerciales (services d'applications mobiles, vente en ligne) et non commerciales (études statistiques, services sanitaires et sociaux). Toutefois, un profilage plus approfondi s'accompagne de risques proportionnels pour les personnes. Lorsque le profilage est à la base d'une décision qui affecte considérablement une personne, une fausse prédiction comporte un risque élevé de préjudice. Comme la vie quotidienne des Ontariens est de plus en plus partagée et gérée par des plates-formes en ligne, il y a plus de données disponibles pour créer des profils, et des risques plus élevés pour la vie privée des citoyens. Lorsque des données profilées sont utilisées avec l'IA pour prendre des décisions concernant des personnes, par exemple des décisions en matière d'emploi, cela devient une forme de « prise de décision automatisée », que l'Ontario propose de définir de la façon suivante :

> « système décisionnel automatisé » 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.

Ces systèmes décisionnels automatisés (ou « SDA ») sont maintenant fréquemment utilisés dans le monde entier pour évaluer l'admissibilité à des programmes, évaluer des candidats à des emplois et commercialiser des produits en fonction des préférences des utilisateurs. Lorsqu'elles sont utilisées pour automatiser des processus répétitifs et structurés, les technologies de SDA aident à la fois les personnes et les entreprises en rendant plus efficaces les décisions impliquant de grands volumes de données. Le risque de préjudice et de discrimination augmente toutefois lorsque ces technologies sont utilisées pour prendre des décisions qui impliquent des données personnelles sensibles ou qui pourraient avoir un impact significatif sur un individu. À ce jour, l'utilisation des SDA est obscure; les gens n'ont qu'une connaissance limitée de la technologie utilisée et n'ont aucun recours pour résoudre les problèmes qui surviennent lorsque les SDA sont utilisés sans une supervision humaine adéquate.

Comme nous l'avons déjà noté, de nombreux territoires ont déjà pris des mesures pour équilibrer l'utilisation de ces technologies avec les droits individuels. Le RGPD européen donne aux individus le droit de ne pas être soumis aux SDA pour des catégories de données sensibles, ou lorsque les décisions pourraient produire des résultats juridiques ou d'autres résultats significatifs. Il permet également aux personnes de contester les décisions de SDA dans ces situations et de demander un examen humain.

Parmi les territoires canadiens qui ont récemment emboîté le pas, citons le Québec, dont le projet de loi 64 donnerait aux individus le droit d'être informés des décisions relatives aux SDA, y compris des raisons et des principaux facteurs et paramètres qui ont conduit à la décision, et la possibilité de soumettre des observations à une personne de l'organisation qui est en mesure d'examiner la décision. De plus, le projet de loi C-11 obligerait les entreprises à fournir un compte rendu de leur utilisation des SDA et, sur demande, une explication de l'incidence des SDA sur une décision particulière.

Ces garde-fous pour les SDA marquent une étape importante dans la protection des personnes et la prévention des pratiques préjudiciables, tout en permettant aux organisations de continuer à utiliser l'IA de manière responsable. L'Ontario envisage de renforcer ces protections, en commençant par la disposition suivante :

> **Système décisionnel automatisé**
> (3) Si l'organisation a utilisé un système décisionnel automatisé pour faire une prédiction, formuler une recommandation ou prendre une décision concernant le particulier, elle lui fournit, à sa demande, une explication de la prédiction, de la recommandation ou de la décision et lui indique la provenance des renseignements personnels utilisés pour faire la prédiction, formuler la recommandation ou prendre la décision.

Il est important de fournir des renseignements clairs sur l'utilisation des SDA; toutefois, les explications ne suffisent pas à redonner le contrôle aux Ontariens. Les individus doivent également être protégés de ces systèmes lorsque leur utilisation pourrait leur causer du tort. Les décisions prises à l'aide de SDA, par exemple dans le cadre d'un emploi, d'une assurance ou d'un service de santé, peuvent avoir de graves conséquences, c'est-à-dire causer un préjudice juridique ou financier, porter atteinte à la réputation ou même mettre en danger la santé et la sécurité. L'Ontario envisage de suivre le modèle du RGPD pour interdire l'utilisation des SDA dans les situations ayant des répercussions *importantes*, sous réserve de certaines exceptions importantes :

> **Interdiction : décision au moyen d'un système décisionnel automatisé**
> (1) L'organisation ne peut utiliser un système décisionnel automatisé, y compris le profilage, pour prendre, au sujet d'un particulier, une décision qui aurait des conséquences importantes pour lui que si, selon le cas :
>
> a) une telle décision est nécessaire pour conclure ou exécuter un contrat entre le particulier et l'organisation;
> b) une telle décision est par ailleurs autorisée en droit;
> c) l'organisation obtient le consentement exprès du particulier quant à l'utilisation d'un système décisionnel automatisé pour prendre une décision qui aurait des conséquences importantes pour lui.

Cette interdiction pourrait fournir des garanties importantes pour les Ontariens et donner aux consommateurs la certitude que leurs données ne peuvent pas être utilisées de manière illimitée. Les entreprises bénéficieraient également de ce niveau accru de certitude et de confiance des consommateurs. Toutefois, cette protection serait incomplète si les Ontariens n'avaient pas le droit de contrôler le processus et d'y participer, c'est-à-dire de comprendre la signification et l'impact d'une décision et d'intervenir dans la décision si elle risque de compromettre leurs intérêts ou leur bien-être. À cet égard, l'Ontario envisage de donner plus de contrôle aux Ontariens par le biais des exigences suivantes :

> **Idem**
> (2) Si l'organisation a utilisé un système décisionnel automatisé pour prendre une décision à laquelle le paragraphe (1) s'appliquerait au sujet d'un particulier, ce dernier peut prendre n'importe laquelle des mesures suivantes :
>
> 1. Demander les renseignements personnels qui ont été utilisés pour prendre la décision.
> 2. Demander les motifs et les principaux facteurs et paramètres qui ont mené à la décision.
> 3. Demander la correction des renseignements personnels qui ont été utilisés pour prendre la décision.

4. Commenter la décision.
5. Contester la décision.
6. Demander la révision de la décision par un particulier au sein de l'organisation ayant les connaissances suffisantes pour le faire.

Une meilleure connaissance et un meilleur contrôle de l'utilisation de leurs données par les SDA pourraient permettre un équilibre des pouvoirs plus juste et plus proportionné entre les personnes et les organisations et garantir que ces protections sont interopérables avec celles d'autres territoires de compétence. Afin d'améliorer la réactivité des organisations aux demandes des particuliers et de renforcer la responsabilisation, l'Ontario pourrait également envisager d'imposer des exigences plus détaillées en matière de tenue de dossiers concernant l'utilisation des SDA, par exemple en exigeant des organisations qu'elles consignent et retracent la collecte et l'utilisation des renseignements personnels dans ce contexte. Étant donné que cette exigence de tenue de registres ajouterait presque certainement un fardeau supplémentaire pour les organisations, la province souhaite recevoir des commentaires sur son utilité et son caractère pratique, ainsi que sur tout autre facteur - comme la taille ou l'échelle de l'organisation ou la sensibilité des renseignements - qui pourrait influencer son application et son inclusion éventuelle dans la loi. Bien que les technologies d'apprentissage automatique ne se limitent pas au profilage et au SDA, ces droits pourraient constituer une base sur laquelle l'Ontario pourrait continuer à élaborer un régime de gouvernance de l'IA plus détaillé et plus complet.

Questions de discussion :

- Les exemples de dispositions fournis dans cette section offrent-ils une protection adéquate aux Ontariens dont les renseignements sont soumis aux pratiques des SDA ?
- L'approche réglementaire proposée pour les SDA permet-elle de trouver le bon équilibre pour renforcer la protection de la vie privée, tout en permettant de nouvelles formes d'innovation socialement bénéfiques dans le domaine de l'IA ?
- Devrait-il y avoir des exigences supplémentaires en matière de tenue de registres ou de traçabilité pour garantir que les organisations restent responsables de leurs pratiques de SDA ?
- Y a-t-il des exigences ou des protections supplémentaires que l'Ontario pourrait envisager en ce qui concerne l'utilisation du profilage ?

Améliorer le consentement et les autres utilisations licites des renseignements personnels

Problème :

Bien que le consentement individuel à la collecte, à l'utilisation ou à la divulgation des renseignements personnels soit une composante essentielle des lois sur la protection de la vie privée, il est largement reconnu que le paysage moderne des données est désormais trop complexe pour s'y fier comme seule autorité pour ces pratiques. La complexité de l'écosystème moderne des données remet également en question la compréhension et la capacité des personnes à consentir, ce qui entraîne souvent une lassitude du consentement, c'est-à-dire un consentement donné, mais non éclairé. Le projet de loi C-11 et le projet de loi 64 du Québec reconnaissent tous deux cette situation. Ils améliorent les processus de consentement tout en prévoyant - comme le font déjà les lois existantes sur la protection de la vie privée - des exceptions au consentement. Toutefois, les propositions du projet de loi C-11 pourraient ne pas protéger adéquatement les Ontariens; par conséquent, l'Ontario envisage les améliorations énoncées ci-dessous.

Objectif :

L'Ontario pourrait améliorer la signification du consentement en le rendant plus éclairé, tout en prévoyant d'autres pouvoirs pour la collecte et l'utilisation des renseignements personnels, afin de réduire la lassitude à l'égard du consentement et de faire en sorte que les organisations ne puissent pas utiliser des consentements individuels non éclairés pour exploiter les données des citoyens.

*

L'un des éléments fondamentaux d'une loi sur la protection de la vie privée est le cadre d'autorité autorisant les organisations à collecter, utiliser et divulguer les données personnelles des individus. Les lois sur la protection de la vie privée autorisent généralement les organisations à ne recueillir que les renseignements personnels nécessaires pour atteindre des objectifs légitimes et déclarés (ce point a également été abordé ci-dessus dans la section « Une approche de la vie privée fondée sur les droits »). Dans la législation canadienne sur la protection de la vie privée, et dans le projet de loi C-11, le consentement de la personne est la principale base juridique sur laquelle les organisations peuvent s'appuyer pour traiter les données personnelles. Ces lois prévoient également des exceptions pour les situations où l'obtention du consentement n'est pas possible ou nécessaire.

Le renforcement de l'autorité du consentement est une première étape importante dans l'élaboration de ce cadre de protection de la vie privée. Toutefois, si le consentement est

un élément important de la protection de la vie privée, les cadres fondés sur le consentement posent également leurs propres défis et limites. Par exemple, les exigences générales en matière de consentement entraînent la prolifération de mentions légales et de politiques de confidentialité denses. Il en résulte une « lassitude du consentement », c'est-à-dire que les personnes cliquent sur « Accepter » les mentions légales qu'elles reçoivent lorsqu'elles s'inscrivent à un service, sans lire ni comprendre les conditions qu'elles acceptent. Ce phénomène est exacerbé par le fait que de nombreux avis de confidentialité sont longs, légalistes et compliqués. Certaines organisations peuvent utiliser des avis rédigés en termes denses pour dissimuler des autorisations d'utilisations secondaires et obtenir la permission de pratiques injustes et inappropriées, auxquelles de nombreux Ontariens ne s'attendraient pas raisonnablement. Les Ontariens pourraient à juste titre s'opposer à de telles clauses s'ils pouvaient comprendre pleinement les risques et les conséquences correspondants, mais ils ne reçoivent pas les informations dont ils ont besoin pour les comprendre vraiment.

Pour contrer ces risques d'utilisation abusive du consentement, une loi ontarienne sur la protection de la vie privée pourrait stipuler que les organisations doivent fournir certains renseignements pour que le consentement soit considéré comme valide; ces exigences potentielles seront décrites dans la prochaine section sur la transparence. L'Ontario pourrait également prévoir le droit de retirer le consentement, exiger que l'on tienne compte du caractère sensible au moment de déterminer la forme du consentement et interdire aux organisations de faire du consentement une condition d'obtention d'un service ou de l'obtenir par des moyens trompeurs ou frauduleux. Ces exigences, si elles sont introduites, seraient conformes à celles prévues dans le projet de loi C-11 proposé par le Canada.

Dans le paysage numérique moderne d'aujourd'hui, où les données sont continuellement recueillies et où les flux d'information sont complexes, l'Ontario a besoin d'autorités alternatives, protégeant la vie privée, pour recueillir et utiliser les renseignements personnels. Dans le projet de loi C-11, ces solutions de rechange sont formulées comme des exceptions au consentement, qui demeure l'autorité centrale par défaut. L'Ontario envisage de formuler ces exceptions comme des cas dans lesquels les renseignements personnels peuvent être recueillis, utilisés ou divulgués comme solutions de rechange au consentement.

Avant de passer à ces solutions de rechange, il faut noter que, comme c'est le cas en vertu des lois canadiennes actuelles sur la protection de la vie privée, l'Ontario envisage de permettre aux organisations de s'appuyer sur le consentement implicite dans certaines circonstances, en tenant compte de la sensibilité des renseignements

personnels en cause et des attentes raisonnables de la personne. Cela contribuerait également à réduire la « lassitude du consentement » pour les Ontariens.

En outre, les personnes ne seraient pas tenues de donner leur consentement pour la collecte, l'utilisation ou la divulgation des renseignements personnels au-delà de ce qui est nécessaire pour recevoir un service ou un produit, et auraient également la possibilité de retirer leur consentement en donnant un avis à l'organisation concernée.

Bon nombre des motifs possibles décrits ci-dessous pour la collecte, l'utilisation et la communication de renseignements personnels sans exiger de consentement sont déjà courants dans les lois canadiennes sur la protection de la vie privée, bien qu'ils soient maintenant généralement formulés comme des « exceptions au consentement ». Les motifs proposés ci-dessous sont aussi généralement conformes à ceux prévus dans le projet de loi C-11, même si, comme on le verra plus loin, ils pouvaient être améliorés par rapport au projet de loi C-11.

> **Activités commerciales**
> (1) L'organisation peut recueillir ou utiliser les renseignements personnels d'un particulier si la collecte ou l'utilisation est faite en vue d'une activité commerciale visée au paragraphe (2) et que, à la fois :
>
> a) une personne raisonnable s'attendrait à une telle collecte ou à une telle utilisation pour cette activité;
> b) les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions du particulier.
>
> **Activités visées**
> (2) Sous réserve des règlements, sont des activités commerciales pour l'application du paragraphe (1) :
>
> 1. Les activités nécessaires à la fourniture ou à la livraison d'un produit ou à la prestation d'un service demandé par le particulier à l'organisation.
> 2. Les activités menées à des fins de diligence raisonnable pour réduire ou prévenir les risques commerciaux de l'organisation.
> 3. Les activités nécessaires à la sécurité de l'information, des systèmes ou des réseaux de l'organisation.
> 4. Les activités nécessaires pour assurer la sécurité d'un produit que l'organisation fournit ou livre ou d'un service qu'elle fournit.
> 5. Les autres activités prescrites.

La liste potentielle d'activités décrite ci-dessus est très similaire à celle prévue dans le projet de loi C-11. Toutefois, l'Ontario est préoccupé par le traitement des dispositions qui ont fait l'objet de critiques dans le projet de loi fédéral. Plus précisément, le projet de

loi C-11 inclut ce qui suit parmi les activités commerciales autorisées : « une activité au cours de laquelle il serait impossible d'obtenir le consentement de la personne parce que l'organisation n'a pas de relation directe avec elle ». Si elle est adoptée, cette disposition du projet de loi C-11 pourrait permettre aux entreprises de recueillir et d'utiliser les données des Ontariens sans leur consentement, simplement pour des raisons de commodité ou d'opportunité.

Par conséquent, le gouvernement envisage d'omettre cette catégorie particulière autorisée de collecte, d'utilisation et de communication. De même, les experts ont également exprimé des inquiétudes quant à la possibilité de permettre l'ajout de « toute autre activité prescrite » (voir (2)5 ci-dessus) par règlement plutôt que par modification législative, en soulignant que cela pourrait également diluer la force des protections. Le gouvernement souhaite recevoir des commentaires sur cette proposition, ainsi que sur la liste des autres activités, afin de s'assurer qu'elles sont bien délimitées et qu'elles ne créent pas de conséquences involontaires qui pourraient affaiblir les protections des Ontariens.

La liste des catégories autorisées se poursuit comme suit :

Opérations commerciales éventuelles
(1) Les organisations qui seront parties à une éventuelle opération commerciale peuvent utiliser et divulguer les renseignements personnels d'un particulier si, à la fois :

a) les renseignements personnels sont dépersonnalisés avant l'utilisation ou la divulgation et le demeurent jusqu'à ce que l'opération soit effectuée;
b) les organisations ont conclu un accord aux termes duquel l'organisation recevant les renseignements s'est engagée :
   (i) à ne les utiliser et à ne les divulguer qu'à des fins liées à l'opération,
   (ii) à les protéger au moyen de mesures de sécurité correspondant à leur volume, à leur nature et à leur caractère délicat,
   (iii) si l'opération n'a pas lieu, à les remettre à l'organisation qui les lui a divulgués ou à procéder à leur élimination, dans un délai raisonnable;
c) les organisations se conforment à l'accord visé à l'alinéa b);
d) les renseignements sont nécessaires :
   (i) pour décider si l'opération aura lieu,
   (ii) s'il est décidé que l'opération aura lieu, pour l'effectuer.

Opération commerciale effectuée
(2) Si l'opération commerciale est effectuée, les organisations y étant parties peuvent utiliser et divulguer les renseignements personnels mentionnés au paragraphe (1) si, à la fois :

a) elles ont conclu un accord aux termes duquel chacune d'elles s'est engagée :
   (i) à n'utiliser et ne divulguer les renseignements personnels dont elles ont le contrôle qu'aux fins auxquelles ils ont été recueillis ou auxquelles il était permis de les utiliser ou de les divulguer avant que l'opération ne soit effectuée,
   (ii) à les protéger au moyen de mesures de sécurité correspondant à leur caractère délicat,
   (iii) à donner effet à tout retrait de consentement;
b) les organisations se conforment à l'accord visé à l'alinéa a);
c) les renseignements sont nécessaires à la poursuite de l'entreprise ou des activités faisant l'objet de l'opération;
d) dans un délai raisonnable après que l'opération a été effectuée, l'une des parties avise le particulier du fait que l'opération a été effectuée et que ses renseignements personnels ont été divulgués en vertu du paragraphe (1).

Exception
(2) Les paragraphes (1) et (2) ne s'appliquent pas à une opération commerciale dont le but premier ou le résultat escompté est l'achat, la vente ou l'autre acquisition, élimination ou location de renseignements personnels.

Divulgation à un fournisseur de services
(1) L'organisation peut divulguer à un fournisseur de services les renseignements personnels d'un particulier.

Utilisation par le fournisseur de services
(2) Le fournisseur de services à qui des renseignements personnels ont été transférés par une organisation ne peut les utiliser qu'aux mêmes fins pour lesquelles l'organisation les a recueillis.

Renseignements dépersonnalisés
L'organisation peut utiliser les renseignements personnels d'un particulier afin de les dépersonnaliser.

Recherche et développement
L'organisation peut utiliser les renseignements personnels d'un particulier à des fins de recherche et de développement internes, s'ils sont dépersonnalisés avant leur utilisation.

Collecte, utilisation ou divulgation autorisée ou exigée par la loi
L'organisation peut recueillir, utiliser ou divulguer les renseignements personnels d'un particulier si la collecte, l'utilisation ou la divulgation, selon le cas, est autorisée ou exigée par une loi ou un règlement de l'Ontario ou du Canada.

Divulgation à un organisme chargé de l'exécution de la loi
L'organisation peut divulguer les renseignements personnels d'un particulier à un organisme chargé de l'exécution de la loi au Canada s'il existe des motifs raisonnables de croire qu'une infraction a été commise et que la divulgation permettrait à l'organisme d'établir s'il y a lieu de mener une enquête à ce sujet.

Enquête ou instance judiciaire
L'organisation peut recueillir, utiliser ou divulguer les renseignements personnels d'un particulier si la collecte, l'utilisation ou la divulgation est raisonnable aux fins d'une enquête ou d'une instance judiciaire.

Collecte de renseignements personnels sur l'employé
L'organisation peut recueillir, utiliser ou divulguer les renseignements personnels d'un employé s'ils sont recueillis, utilisés ou divulgués uniquement aux fins suivantes :

a) établir ou gérer une relation d'emploi ou une relation de travail bénévole entre l'organisation et le particulier, ou y mettre fin;
b) gérer une relation postérieure à un emploi ou à un travail bénévole entre l'organisation et le particulier.

Collecte par une association négociatrice concernant une obligation prévue par une convention collective
Une association négociatrice peut recueillir, utiliser ou divulguer des renseignements personnels concernant un employé si la collecte, l'utilisation ou la divulgation est nécessaire, selon le cas :

a) dans le cadre d'une campagne d'acquisition du droit à la négociation collective;
b) pour respecter une obligation prévue par une convention collective ou pour traiter d'un litige découlant de la convention collective;
c) afin de représenter des employés en ce qui a trait à leurs conditions d'emploi.

Collecte par une association négociatrice concernant un conflit de travail
Une association négociatrice peut recueillir, utiliser ou divulguer des renseignements personnels concernant un particulier afin d'informer ou de

persuader le public sur une question d'intérêt public ou de grande importance concernant un conflit de travail impliquant l'association négociatrice.

Intérêt du particulier
L'organisation peut recueillir ou utiliser les renseignements personnels d'un particulier lorsque la collecte ou l'utilisation est manifestement dans l'intérêt du particulier, mais uniquement si l'obtention du consentement est difficilement réalisable.

Situation d'urgence
L'organisation peut utiliser ou divulguer les renseignements personnels d'un particulier lorsque cela est nécessaire pour intervenir face à une situation d'urgence qui met en danger la santé ou la sécurité d'un particulier ou du public. Si le particulier que concernent les renseignements est en vie, l'organisation l'informe de la divulgation par écrit et sans délai.

Identification d'un particulier
L'organisation peut divulguer les renseignements personnels d'un particulier lorsque la divulgation est nécessaire aux fins d'identification du particulier qui est blessé, malade ou décédé et qu'elle est faite à une institution gouvernementale ou à une subdivision d'une telle institution, au plus proche parent du particulier ou à son représentant autorisé. Si le particulier est en vie, l'organisation doit l'informer de la divulgation par écrit et sans délai.

Divulgation : plus proche parent ou représentant autorisé
L'organisation peut divulguer les renseignements personnels d'un particulier à une institution gouvernementale ou à une subdivision d'une telle institution qui les a demandés en mentionnant la source de l'autorité légitime étayant son droit de les obtenir et le fait que la divulgation est faite afin d'entrer en contact avec le plus proche parent d'un particulier blessé, malade ou décédé, ou avec son représentant autorisé.

Recherche dans l'intérêt public
L'organisation peut utiliser ou divulguer les renseignements personnels d'un particulier à des fins de recherche s'il est satisfait à toutes les conditions suivantes :

1. Les fins de la recherche ne peuvent être réalisées sans que les renseignements ne soient utilisés ou divulgués, selon le cas.
2. Les fins de la recherche portent sur une question d'intérêt public.
3. L'utilisation ou la divulgation n'est pas susceptible de nuire au particulier.
4. La recherche ne vise pas à prendre des décisions concernant des particuliers.

5. Les résultats de la recherche seront rendus publics, mais pas sous une forme qui pourrait raisonnablement permettre d'identifier un particulier.
6. L'obtention du consentement est difficilement réalisable.
7. L'organisation informe le commissaire de l'utilisation ou de la divulgation avant de divulguer les renseignements.
8. Les autres conditions prescrites.

Documents ayant une valeur historique ou archivistique
L'organisation peut divulguer les renseignements personnels d'un particulier à une entité dont les fonctions comprennent la conservation des documents ayant une valeur historique ou archivistique, si la divulgation est faite en vue d'une telle conservation.

Atteinte aux mesures de sécurité
L'organisation peut divulguer les renseignements personnels d'un particulier à son insu ou sans son consentement si, à la fois :

a) la divulgation est faite à l'autre organisation, ou à l'institution gouvernementale ou subdivision d'une telle institution qui a été avisée de l'atteinte;
b) la divulgation n'est faite que pour réduire le risque de préjudice pour le particulier qui pourrait résulter de l'atteinte ou atténuer ce préjudice.

Divulgation après une période de temps
L'organisation peut divulguer les renseignements personnels d'un particulier après celle des périodes suivantes qui se termine la première :

a) 100 ans après la création du document les contenant;
b) 30 ans après le décès du particulier.

Renseignements mis à la disposition du public
L'organisation peut recueillir et utiliser les renseignements personnels d'un particulier, si les renseignements 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 du particulier.

Deux des motifs susmentionnés nécessitent une attention particulière : la collecte de renseignements personnels sur l'employé et la collecte, l'utilisation et la divulgation des renseignements personnels par un syndicat.

Les employeurs ont l'obligation légale de recueillir, d'utiliser et de divulguer les renseignements personnels concernant les employés, y compris à des fins fiscales. Par conséquent, il n'est pas possible d'exiger le consentement pour la collecte, l'utilisation et

la divulgation des renseignements personnels des employés lorsqu'ils sont liés à l'établissement et à la gestion d'une relation employeur-employé. Cela ne signifie pas pour autant que les employeurs auraient le champ libre. Comme c'est le cas dans les lois canadiennes actuelles sur la protection de la vie privée, l'Ontario pourrait prévoir que la collecte de renseignements personnels sur les employés doit être nécessaire à la relation d'emploi et que les employés doivent être avisés lorsque la collecte a lieu. Toute collecte de renseignements personnels au-delà de ce qui est nécessaire pour établir ou gérer la relation employeur-employé ne serait donc pas autorisée par ce pouvoir légal. Par exemple, si un employeur voulait recueillir des informations socio-économiques sur les employés à des fins de planification de la diversité et de l'inclusion, il devrait obtenir le consentement de l'employé concerné.

De même, les syndicats ont des obligations légales à l'égard des membres du syndicat qui seraient grandement entravées si l'on devait exiger le consentement du travailleur individuel pour recueillir, utiliser et divulguer ces renseignements personnels à des fins légitimes. Comme l'a affirmé la Cour suprême du Canada relativement à la loi albertaine sur la protection de la vie privée dans le secteur privé, les syndicats utilisent les renseignements personnels pour remplir un rôle unique de représentation en milieu de travail et dans la société. Les autres motifs décrits ci-dessus pourraient permettre aux organisations de négociation, qui seraient définies de manière à inclure les syndicats et toute association d'employés agissant dans le domaine des conditions d'emploi, de recueillir, d'utiliser et de communiquer des renseignements personnels pour s'acquitter de leurs obligations légitimes. Cette définition permettrait aux organisations qui cherchent à devenir un syndicat accrédité de s'appuyer également sur ce pouvoir pour la collecte, l'utilisation et la communication de renseignements personnels. Ce pouvoir permettrait aux syndicats de mener leurs activités légitimes sans entrave, tout en assurant une meilleure protection des renseignements personnels des travailleurs.

Bien que l'Ontario reconnaisse le consentement comme une autorité centrale et significative, ces bases alternatives potentielles pourraient contribuer à faire en sorte que les Ontariens n'aient pas à supporter tout le fardeau de contrôler les pratiques en matière de données et de demander des comptes aux organisations. Cela vise à responsabiliser les Ontariens en veillant à ce que le consentement, le cas échéant, ne soit pas simplement une case à cocher, mais une autorisation significative et éclairée des individus à exercer un plus grand contrôle sur leurs données. Il convient également de noter que le critère de finalité « juste et appropriée « exposé dans la première section du présent document continuerait de s'appliquer à chaque cas autorisé de collecte, d'utilisation et de communication, quelles que soient les autres autorisations qui pourraient également s'appliquer.

Questions de discussion :

- La liste type des « catégories autorisées » fournit-elle un ensemble suffisant d'autorisations pour la collecte, l'utilisation et la divulgation des informations personnelles ? Y a-t-il des catégories manquantes ? Y a-t-il des catégories qui sont trop permissives ?
- Examinez l'exemple de disposition sur les « activités commerciales « fourni ci-dessus. Est-elle bien équilibrée pour protéger les renseignements personnels tout en permettant aux entreprises de mener leurs activités ? Comment l'Ontario devrait-il définir le concept de « risque commercial » ? Est-ce que « toute autre activité prescrite » devrait être retirée de la liste des activités commerciales ?
- Y a-t-il des protections ou des exigences supplémentaires que l'Ontario devrait envisager à l'égard des fournisseurs de services ?

Transparence des données pour les Ontariens

Problème :

La plupart des pratiques en matière de données sont désormais opaques et beaucoup trop complexes pour que l'Ontarien moyen puisse les suivre. Cette opacité peut amener les citoyens à consentir à des pratiques qui créent des risques dont ils ne sont pas conscients. Elle peut également susciter la méfiance à l'égard des organisations, et donc risquer de nuire à l'innovation commerciale si les personnes croient que leurs renseignements sont exploités de manière obscure. Comme l'a souligné la commissaire à l'information et à la protection de la vie privée de l'Ontario dans ses observations lors de la consultation de 2020 sur la réforme de la protection de la vie privée en Ontario, « la transparence est une composante essentielle de tout cadre de protection de la vie privée dans le secteur privé et devrait en être un des principes les plus importants ». Pour ces raisons, les lois modernes sur la protection de la vie privée exigent des organisations une transparence significative sur leurs pratiques en matière de données.

Objectif :

Des exigences de transparence plus strictes pourraient donner aux citoyens le droit de savoir quand et comment leurs données sont utilisées par les organisations, ce qui leur permettrait de reprendre le contrôle et de participer de manière plus significative aux décisions qui affectent leur bien-être.

*

La transparence est une pierre angulaire du droit moderne de la vie privée. Le droit à la vie privée ne peut avoir de sens que si les personnes disposent des connaissances nécessaires pour l'exercer. Les flux et les utilisations des renseignements personnels

sont désormais si complexes qu'il est impossible pour la plupart des Ontariens de suivre la multitude de collectes et de transferts, ou de comprendre comment leurs données sont utilisées une fois qu'elles sont sous la garde d'une organisation. Au cours de la consultation sur la réforme de la protection de la vie privée de 2020, les Ontariens et les entreprises ont tous indiqué que des règles et des explications en langage clair et simple sont essentielles à l'établissement d'une culture de protection de la vie privée dans ce paysage de données complexe.

D'autres territoires ont fait quelques avancées dans ce domaine. Le RGPD exige des organisations qu'elles fournissent des informations concises, intelligibles et facilement accessibles aux individus tout au long du cycle de vie du traitement de leurs données**.** Le projet de loi 64 du Québec renforce les exigences de transparence, et le projet de loi C-11 prévoit que les organisations doivent fournir des politiques et des pratiques en langage clair aux personnes. Cela comprend l'obligation de fournir des détails sur l'utilisation des renseignements personnels, sur les organisations avec lesquelles ils sont partagés et sur la durée de leur conservation. Le projet de loi C-11 permet toutefois aux organisations de recueillir et d'utiliser des renseignements personnels à diverses fins sans avoir à en informer les personnes concernées.

L'Ontario étudie comment adapter et améliorer les règles de transparence en vigueur dans d'autres territoires. Deux propositions sont à l'étude.

La première proposition serait d'exiger des organisations qu'elles mettent en œuvre des politiques, des pratiques et des procédures internes en matière de protection de la vie privée. En d'autres termes, elles pourraient être tenues de mettre en œuvre un programme de gestion de la vie privée pour régir leur collecte, leur utilisation et leur communication de renseignements personnels, et de rendre ce programme accessible pour examen. Cela permettrait de s'assurer que les employés de l'organisation connaissent le programme et s'y conforment. Entre autres choses, les employés seraient plus réceptifs aux demandes d'information et aux demandes de renseignements des membres du public. Ces programmes de gestion de la protection de la vie privée s'appuieraient sur des ressources et des modèles élaborés par la province et seraient également mis à la disposition, sur demande, de l'organisme de réglementation de la protection de la vie privée de l'Ontario, le commissaire à l'information et à la protection de la vie privée de l'Ontario.

> **Programme de gestion de la protection des renseignements personnels**
> (1) L'organisation met en œuvre un programme de gestion de la protection des renseignements personnels qui comprend les politiques, les pratiques et les procédures qu'elle a mises en place afin de respecter les obligations qui lui incombent sous le régime de la présente loi, notamment des politiques, des pratiques et des procédures relatives :

a) à la protection des renseignements personnels;
b) à la réception des demandes de renseignements et des plaintes et à leur traitement;
c) à la formation et aux renseignements fournis à son personnel relativement à ses politiques, à ses pratiques et à ses procédures;
d) à l'élaboration de contenu expliquant les politiques, les pratiques et les procédures qu'elle a mises en place afin de respecter les obligations qui lui incombent sous le régime de la présente loi.

L'obligation pour les organisations de mettre en œuvre un programme de gestion de la protection des renseignements personnels sera modulable en fonction de la taille de l'organisation. Lors de l'élaboration d'un programme de gestion de la protection des renseignements personnels, les organisations tiendront compte du volume, de la nature et de la sensibilité des renseignements personnels dont elles ont la charge. Ainsi, les petites organisations qui ne recueillent pas de renseignements personnels très sensibles ne seront pas tenues d'élaborer des politiques et des procédures complexes de la protection des renseignements personnels. De même, les grandes organisations qui collectent, utilisent et divulguent de grandes quantités de renseignements personnels (y compris des informations très sensibles) devront disposer d'un programme de gestion de la protection des renseignements personnels solide et adapté à l'ampleur du traitement des données qu'elles entreprennent.

Outre l'exigence susmentionnée, le libellé proposé ci-dessous en matière de transparence garantirait une transparence externe en obligeant les organisations à rendre facilement accessibles les informations relatives à leurs politiques, pratiques et procédures en matière de conformité. La deuxième amélioration proposée en matière de transparence (décrite ci-dessous) concerne l'envoi d'avis aux personnes à qui l'on demande de consentir à la collecte de leurs renseignements personnels.

La transparence dans l'obtention du consentement est importante, car il s'agit d'un moyen essentiel pour les individus d'avoir un certain contrôle sur leurs renseignements personnels. Toutefois, comme indiqué plus haut, les avis de consentement peuvent submerger les individus au lieu de les responsabiliser. Des informations excessivement denses et compliquées peuvent donc éroder la validité du consentement. Elle peut également miner l'efficacité d'autres droits relatifs aux données. Les commentaires recueillis lors des consultations sur la réforme de la protection de la vie privée de l'Ontario en 2020 ont mis en évidence cette préoccupation, c'est-à-dire que l'accessibilité des avis de consentement et les exigences en matière de langage clair et simple sont importantes pour faire en sorte que l'information soit significative et contribue à la capacité des Ontariens de prendre des décisions éclairées.

C’est pourquoi, au lieu d’inonder les citoyens de politiques de protection de la vie privée longues et mal rédigées ou de notifications difficiles à trouver, l’Ontario envisage d’obliger les organisations à mettre à disposition des informations, en langage clair, qui expliquent comment l’organisation utilise les données des individus, sur quelle base légale elle s’appuie et comment les Ontariens peuvent faire le suivi pour exercer leurs droits en matière de données.

Cette proposition comporte deux aspects. Le premier est l’obligation, mentionnée ci-dessus, pour les organisations de mettre à disposition des informations sur leurs politiques, pratiques et procédures en matière de conformité. Un élément de cette proposition serait directement lié au consentement éclairé :

> **Politiques, pratiques et procédures**
> (1) L’organisation rend facilement accessibles, dans un langage clair, des renseignements sur les politiques, les pratiques et les procédures qu’elle a mises en place afin de respecter les obligations qui lui incombent sous le régime de la présente loi.
>
> **Renseignements supplémentaires**
> (2) Pour respecter l’obligation prévue au paragraphe (1), l’organisation rend facilement accessibles les renseignements suivants :
>
> 1. La description du type de renseignements personnels qu’elle recueille et les fins particulières pour lesquelles ils le sont.
> 2. Une explication générale de la façon dont l’organisation utilise ou divulgue les renseignements personnels.
> 3. Si l’organisation ne se fonde pas sur le consentement du particulier pour l’utilisation ou la divulgation, la description des catégories énoncées aux articles xx à xx sur lesquelles elle s’appuie pour l’utilisation ou la divulgation.
> 4. Une explication générale de l’usage qu’elle fait des systèmes décisionnels automatisés pour faire des prédictions, formuler des recommandations ou prendre des décisions à l’égard des particuliers qui pourraient avoir une incidence importante sur eux ainsi que l’énoncé des droits du particulier à l’égard du système décisionnel automatisé.
> 5. La manière dont un particulier peut présenter une demande d’élimination de renseignements personnels ou une demande d’accès aux renseignements personnels.
> 6. Les coordonnées du particulier à qui les demandes de renseignements ou les plaintes peuvent être adressées.

L’une des principales caractéristiques de la proposition susmentionnée est que la transparence des organisations concernant leurs utilisations et leurs divulgations de

renseignements personnels ne serait pas limitée aux situations où les personnes donnent leur consentement. Le projet de loi C-11 contient des exigences de transparence similaires, mais la proposition de l'Ontario renforcerait la transparence en exigeant plus de détails sur la collecte, l'utilisation et la divulgation des informations.

En ce qui concerne l'établissement d'un programme de gestion de la protection des renseignements personnels et de politiques de protection des renseignements personnels, le projet de loi 64 du Québec prévoit également l'obligation pour les organisations de procéder à une évaluation des facteurs liés à la protection des renseignements personnels dans le cadre de tout projet de système d'information ou de prestation de services électroniques comportant des renseignements personnels (c.-à-d. une « évaluation des facteurs relatifs à la vie privée «). De même, le CPVP fédéral a demandé que le projet de loi fédéral C-11 soit modifié afin d'inclure l'obligation pour les organisations de suivre les principes de « protection intégrée de la vie privée » et d'effectuer des évaluations des facteurs relatifs à la vie privée pour les activités à risque élevé. L'approche du Québec et celle du CPVP visent toutes deux à accroître la responsabilité en matière de protection de la vie privée dans les organisations. L'Ontario souhaite recueillir des commentaires afin d'évaluer la valeur de telles exigences pour améliorer la transparence et la responsabilité, ainsi que les répercussions sur les organisations si des exigences similaires étaient introduites dans la province.

Le deuxième aspect de la proposition de l'Ontario, exposé ci-dessous, concerne directement les renseignements qui doivent être fournis par une organisation pour obtenir un consentement valide, reconnaissant que, lorsque le consentement est requis, la transparence joue un rôle important pour assurer sa validité. Les dispositions suivantes illustrent l'approche envisagée par l'Ontario et précisent le type de renseignements qu'une organisation serait tenue de fournir pour obtenir le consentement valide d'une personne :

> **Renseignements nécessaires à la validité du consentement**
> (3) Le consentement du particulier n'est valide que s'il est satisfait aux conditions suivantes :
>
> 1. Il est raisonnable de s'attendre à ce que le particulier comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la divulgation des renseignements personnels auxquelles il a consenti.
> 2. Au plus tard au moment où l'organisation cherche à obtenir le consentement du particulier, elle lui fournit, dans un langage clair, les renseignements suivants :
>
>   i. Le fait que le particulier a le droit de donner, de refuser ou de retirer son consentement conformément à la présente loi.

ii. Les fins de la collecte, de l'utilisation ou de la divulgation des renseignements personnels, établies par l'organisation et consignées.
iii. La façon dont les renseignements personnels seront recueillis, utilisés ou divulgués, notamment si l'organisation utilisera un système décisionnel automatisé à l'égard des renseignements.
iv. Les conséquences raisonnablement prévisibles de la collecte, de l'utilisation ou de la divulgation des renseignements personnels.
v. Le type précis de renseignements personnels qui seront recueillis, utilisés ou divulgués.
vi. Le nom des tiers ou les catégories de tiers auxquels l'organisation peut divulguer les renseignements personnels.

Le principe de transparence est fondamental pour la création d'une société plus protectrice de la vie privée. La commissaire à l'information et à la protection de la vie privée de l'Ontario a souligné dans ses observations que le consentement est éclairé uniquement lorsqu'on peut raisonnablement s'attendre à ce que la personne comprenne la nature, l'objet et les conséquences de ce qu'on lui demande. L'approche envisagée par l'Ontario vise à donner aux Ontariens un plus grand contrôle sur l'utilisation de leurs données en leur permettant d'acquérir des connaissances. Cela leur permettrait ensuite de participer de manière plus significative aux actions, pratiques et décisions qui affectent leur vie quotidienne.

Questions de discussion :

- L'exigence d'un « programme de gestion de la protection des renseignements personnels » est-elle suffisante pour garantir que les organisations sont responsables des renseignements personnels qu'elles recueillent ?
- Les dispositions types de cette section sont-elles suffisantes pour que les Ontariens comprennent la nature, le but et les conséquences de la collecte et de l'utilisation de leurs renseignements personnels par une organisation ?
- L'Ontario devrait-il envisager d'imposer des pratiques de « protection intégrée de la vie privée » ou des « évaluations des facteurs relatifs à la vie privée « ? Ces types d'exigences entraîneraient-ils un fardeau excessif pour les organisations ?

Protéger les enfants et les jeunes

Problème :

Les enfants font partie des groupes les plus vulnérables de l'économie numérique. Leur activité en ligne intensive, combinée à l'obscurité croissante des pratiques en matière de données, en fait des cibles faciles pour une surveillance injustifiée, un suivi invasif et l'influence de mauvais acteurs.

Objectif :

L'Ontario pourrait prévoir des protections spéciales pour les enfants afin de les prémunir contre ces dangers accrus en introduisant un âge minimum de consentement valide et en interdisant aux organisations de surveiller les enfants dans le but d'influencer leurs décisions ou leur comportement.

*

Les risques associés aux pratiques modernes en matière de données sont nettement plus élevés pour les populations vulnérables. Une personne peut être considérée comme vulnérable lorsque les circonstances limitent sa capacité à consentir ou à s'opposer valablement à la collecte, l'utilisation ou la divulgation de ses données, ou lorsqu'il existe un déséquilibre de pouvoir important entre cette personne et l'organisation qui contrôle ses renseignements.

Les enfants et les jeunes représentent un exemple de cette vulnérabilité, en particulier lorsqu'ils participent à des activités virtuelles telles que les jeux, l'apprentissage en ligne ou la publication sur les médias sociaux. Sans protections adéquates, les enfants peuvent être des cibles faciles pour les pratiques d'exploitation des données et les influences comportementales qui peuvent être créées par l'utilisation des technologies modernes de l'information, y compris l'IA.

En plus des protections décrites dans Une approche de la vie privée fondée sur les droits, il existe un certain nombre de domaines dans lesquels l'Ontario envisage des protections supplémentaires pour les enfants et les jeunes. L'Ontario envisage d'introduire une exigence explicite de consentement parental au nom d'un « enfant » de moins de 16 ans. Cela signifierait l'âge du consentement pour la collecte, l'utilisation et la divulgation de renseignements personnels. Cette exigence, qui est similaire à une exigence du RGPD relative à l'activité en ligne des enfants, permettrait de s'assurer que la personne consentante est en mesure de comprendre et de saisir pleinement les détails pertinents, ainsi que les risques et les conséquences possibles.

Grâce à la proposition suivante, l'Ontario pourrait renforcer la responsabilité parentale, une première étape essentielle pour protéger les enfants de l'Ontario contre les pratiques en ligne potentiellement dangereuses :

> **Renseignements personnels d'un enfant**
> (1.1) Dans le cas de la collecte, de l'utilisation ou de la divulgation des renseignements personnels d'un enfant, le consentement doit être donné au nom de l'enfant par une personne qui en a la garde légitime.
>
> **Vérification de l'identité**
> (1.2) Pour l'application du paragraphe (1.1), l'organisation prend des mesures raisonnables pour vérifier l'identité de la personne qui se présente comme ayant la garde légitime de l'enfant et pour vérifier qu'elle en a effectivement la garde légitime.
>
> **Idem**
> (1.3) L'organisation peut demander à un particulier qui se présente comme ayant la garde légitime de l'enfant de lui fournir des renseignements suffisants pour lui permettre de s'acquitter des obligations que lui impose le présent article.

Cette autorité parentale (ou de tuteur) en matière de consentement s'étendrait également à l'exercice des autres droits à la vie privée au nom de l'enfant dont ils ont la garde légale. À l'instar des dispositions de la *Loi sur l'accès à l'information et la protection de la vie privée*, un parent ou un tuteur pourrait demander l'accès aux renseignements personnels de l'enfant. Il peut également demander qu'ils soient corrigés, fournis dans un format lisible par machine, effacés, ou contester les pratiques de gestion de la vie privée de l'organisme en déposant une plainte auprès de l'organisme ou du commissaire à l'information et à la protection de la vie privée de l'Ontario.

De nombreux enfants jouissent d'un degré élevé de liberté et de discrétion lorsqu'ils interagissent avec des plates-formes en ligne. Pour reconnaître la capacité des mineurs matures, l'Ontario pourrait envisager de donner aux jeunes âgés de 13 à 16 ans le droit de s'opposer au consentement de leur parent (ou tuteur) à fournir des renseignements personnels en leur nom ou, inversement, de s'opposer à la demande de leur parent (ou tuteur) de détruire ou de retirer des renseignements personnels les concernant.

Tout comme le consentement parental peut aller à l'encontre de la préférence d'un mineur, il n'est pas toujours suffisant pour protéger les enfants contre les pratiques nuisibles en matière de données. Pour résoudre ce problème, l'Ontario envisage la possibilité d'interdire explicitement aux organisations d'utiliser les technologies d'intelligence artificielle pour exploiter les données des enfants. L'objectif serait d'établir une « zone interdite » pour préciser que les besoins légitimes d'une organisation ne

peuvent inclure la surveillance ou le profilage d'une personne de moins de 16 ans dans le but d'influencer ses décisions ou son comportement.

En plus des protections pour les enfants et les jeunes, il est proposé que, dans le cas des personnes qui sont vulnérables pour d'autres raisons et qui ne peuvent pas exercer leur droit à la vie privée, les règles suivantes puissent s'appliquer :

> **Personnes autorisées**
> (1) Les droits conférés à un particulier par la présente loi peuvent être exercés par :
>
> a) son représentant successoral, dans le cas du particulier décédé, si l'exercice de ce droit ou pouvoir est lié à l'administration de sa succession;
> b) son procureur constitué en vertu d'une procuration perpétuelle, son procureur constitué en vertu d'une procuration relative au soin de la personne, le tuteur à sa personne ou le tuteur à ses biens;
> c) la personne qui a la garde légitime du particulier, si celui-ci est un enfant.
>
> **Besoins légitimes**
> (4) Pour l'application de la disposition 2 du paragraphe (2), les besoins légitimes d'une organisation ne comprennent pas, selon le cas :
>
> a) la surveillance ou le profilage des particuliers âgés de moins de 16 ans dans le but d'influencer leur comportement ou leurs décisions;
> b) les fins dont on sait qu'elles causent, ou qui sont susceptibles de causer, un préjudice grave aux particuliers ou à des groupes de particuliers;
> c) les fins qui contreviendraient à une loi de l'Ontario ou du Canada;
> d) les autres fins prescrites.

Prises ensemble, ces protections supplémentaires pourraient constituer de premières mesures significatives pour garantir la protection du droit à la vie privée des enfants et d'autres personnes vulnérables, et faire en sorte que l'IA ne puisse pas être utilisée à des fins de marketing invasif, de conditionnement ou d'influence comportementale, ou d'une manière qui aurait autrement des effets négatifs sur les jeunes Ontariens. La protection des enfants est importante pour les parents et les familles, et constitue un investissement dans un avenir plus protecteur de la vie privée. Si ces protections sont introduites, le gouvernement de l'Ontario pourrait entreprendre d'autres travaux avec le commissaire à l'information et à la protection de la vie privée de l'Ontario afin d'élaborer des codes de pratique et de conduite supplémentaires qui ressemblent à ceux introduits dans certains territoires européens.

Questions de discussion :

- Quelles sont les considérations supplémentaires à prendre en compte pour déterminer l'âge approprié de consentement à la collecte, l'utilisation et la divulgation de renseignements personnels ?
- Quels défis opérationnels les organisations pourraient-elles rencontrer en incluant des exigences relatives à l'âge du consentement pour la collecte, l'utilisation et la divulgation de renseignements personnels ?
- L'Ontario devrait-il envisager d'autres exigences pour améliorer la protection d'autres populations vulnérables, comme les personnes âgées et les personnes handicapées ?

Un régime réglementaire équitable, proportionné et favorable.

Problème :

Une loi sur la protection de la vie privée serait inefficace sans une surveillance réglementaire. Un organisme de surveillance indépendant est nécessaire pour promouvoir les bonnes pratiques en matière de protection de la vie privée et aussi pour faire appliquer la loi, le cas échéant.

Objectif :

L'Ontario pourrait étendre le mandat du commissaire à l'information et à la protection de la vie privée (CIPVP) de l'Ontario pour y inclure la surveillance et la conformité à ces exigences proposées. Ce mandat pourrait introduire des pouvoirs d'application plus forts pour obliger les organisations à rendre des comptes, tout en permettant au CIPVP de fournir un soutien et des conseils aux organisations.

*****

En tant qu'agent de l'Assemblée législative, le CIPVP de l'Ontario a plus de 30 ans d'expérience dans la surveillance de la conformité des organismes publics aux règles de confidentialité du secteur public de l'Ontario. Le CIPVP a également une longue expérience de la surveillance de la conformité aux règles de protection de la vie privée dans le domaine de la santé, tant dans le secteur public que dans le secteur privé, en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé. Le* CIPVP serait donc le meilleur choix pour assurer la surveillance d'une loi ontarienne sur la protection de la vie privée dans le secteur privé.

Le projet de loi C-11 confère au commissaire à la protection de la vie privée du Canada un rôle de surveillance plus robuste et lui confère une gamme élargie de pouvoirs pour assurer la conformité, notamment des pouvoirs de vérification, d'enquête et

d’ordonnance. Toutefois, il prévoit également des formes de conformité plus favorables, autorisant le commissaire à approuver des programmes de certification et des codes de pratique qui fourniront des lignes directrices claires aux organisations, réduisant ainsi le risque de contraventions. Le projet de loi C-11 propose également de créer un tribunal administratif chargé d’entendre les appels interjetés à la suite de décisions du commissaire et d’imposer des sanctions pécuniaires.

À l’exception du tribunal proposé dans le projet de loi C-11, l’Ontario envisage d’adopter un cadre d’application similaire, en mettant l’accent sur les conseils et le soutien aux organisations. Dans la mesure du possible, des outils et des ressources devraient être mis à la disposition des organisations pour les aider à comprendre leurs obligations en vertu d’une loi sur la protection de la vie privée. À cet égard, le mandat du CIPVP pourrait inclure la réalisation de campagnes de sensibilisation du public et la publication de documents d’orientation, permettant aux organisations de toutes tailles de comprendre les mesures à prendre pour se conformer à la loi. Les orientations et les outils peuvent contribuer à réduire le fardeau des organisations lorsqu’elles intègrent les exigences en matière de protection de la vie privée dans leurs politiques et procédures. Il s’agit d’un rôle que le CIPVP remplit déjà depuis de nombreuses années dans le cadre des lois ontariennes existantes sur la protection de la vie privée.

La certification par le CIPVP des « codes de pratique » est un autre outil proactif et de soutien qui pourrait promouvoir la conformité. Un code de pratique est un ensemble détaillé de principes et d’exigences qu’une organisation, ou un groupe d’organisations (comme un secteur ou une industrie spécifique) élaborent pour répondre aux exigences de la loi. Les programmes de certification, soumis à l’approbation du CIPVP, pourraient également renforcer la confiance en garantissant aux personnes que les pratiques de l’organisation sont conformes à un code de pratique donné et qu’elles gèrent et protègent de manière proactive la vie privée.

Pour être un organe de surveillance efficace, le CIPVP devrait également avoir l’autorité et les ressources nécessaires pour déployer divers outils afin de faire appliquer la loi et d’exiger des organisations qu’elles se conforment à la loi. À cet égard, le CIPVP devrait avoir le pouvoir d’initier et de mener des enquêtes et des audits et d’obliger les organisations à fournir des informations pertinentes sur la manière de gérer les renseignements personnels. Le CIPVP devrait également avoir le pouvoir discrétionnaire de déterminer quand enquêter sur une plainte.

À l’issue d’une enquête, le CIPVP devrait avoir la possibilité d’émettre des ordres contraignants à l’intention des organisations qui se révèlent être en infraction avec la loi. Le pouvoir de donner des ordres pourrait inclure la capacité d’ordonner à une organisation de prendre des mesures pour se conformer à la loi, de cesser de faire quelque chose qui est contraire à la loi, de rendre publiques toutes les mesures qu’elle a

prises pour remplir ses obligations en vertu de la loi, et de détruire toute information personnelle collectée illégalement.

Pour renforcer le cadre de conformité, des sanctions administratives pécuniaires pourraient servir de moyen de dissuasion pour les organisations qui enfreignent les exigences en matière de protection de la vie privée. Dans le contexte ontarien, les sanctions monétaires pourraient être administrées par le CIPVP plutôt que par le tribunal indépendant proposé au niveau fédéral. Les décisions du CIPVP en matière de pénalités seraient soumises à un contrôle judiciaire, comme c'est le cas actuellement pour ses autres décisions judiciaires en vertu des lois ontariennes sur le secteur public.

Pour garantir l'efficacité, le montant de la sanction pourrait tenir compte de l'ampleur du préjudice, de la manière dont l'organisation a tenté de le prévenir ou de l'atténuer, du nombre de personnes qui ont pu être touchées, etc. En outre, le montant de la sanction pourrait tenir compte de la taille de l'organisation et de son revenu annuel global. Cette approche s'aligne sur le projet de loi 64 du Québec, qui propose des sanctions différentes pour les individus et les organisations et qui tient compte de la taille de l'organisation.

> **Décret**
> (1) Si, à l'issue d'une enquête, le commissaire conclut qu'une organisation a contrevenu à la présente loi, il peut, par ordonnance, imposer une pénalité administrative à l'organisation.
>
> **Pénalité administrative : motifs**
> (2) Une personne peut être tenue de payer une pénalité administrative en vertu du présent article pour les motifs suivants :
>
> 1. Afin d'encourager l'observation de la présente loi et de ses règlements.
> 2. Afin d'empêcher quiconque de tirer, directement ou indirectement, un avantage économique par suite d'une contravention à la présente loi ou à ses règlements.
>
> **Facteurs à prendre en compte**
> (3) Lorsqu'il fixe, en application du présent article, le montant de la pénalité administrative pour une contravention, le commissaire peut tenir compte des facteurs suivants et des autres facteurs qu'il estime pertinents :
>
> 1. L'étendue du préjudice ou du préjudice potentiel causé par la contravention.
> 2. Le nombre de particuliers et d'autres personnes touchés par la contravention.
> 3. La mesure dans laquelle la contravention constitue une dérogation aux exigences prévues par la présente loi ou les règlements.

4. La mesure dans laquelle l'organisation aurait pu prendre des mesures pour prévenir la contravention.
5. La mesure dans laquelle l'organisation a tenté d'atténuer tout préjudice ou préjudice potentiel ou de prendre d'autres mesures correctives.
6. La question de savoir si l'organisation a avisé le commissaire et les particuliers dont les renseignements personnels ont été touchés par la contravention.
7. La mesure dans laquelle l'organisation a tiré ou aurait pu raisonnablement s'attendre à tirer, directement ou indirectement, des avantages économiques de la contravention.
8. La question de savoir si l'organisation a déjà contrevenu à la présente loi ou aux règlements.
9. La question de savoir si l'organisation a volontairement fait un versement, à titre de dédommagement, à une personne ou à d'autres particuliers touchés par la contravention.

Contenu de l'ordonnance d'imposition d'une pénalité administrative
(4) L'ordonnance exigeant d'une organisation le paiement d'une pénalité administrative réunit les conditions suivantes :

a) elle contient une description de la contravention ou est accompagnée d'une telle description;
b) elle précise le montant de la pénalité à payer ainsi que le délai et le mode de paiement.

Mesures d'exécution
(5) L'utilisation d'une mesure d'exécution prévue par la présente loi à l'égard d'une contravention à la présente loi ou à ses règlements n'a pas pour effet d'interdire l'utilisation, au même moment ou à des moments différents, des autres mesures d'exécution ou recours prévus par la présente loi ou par ailleurs en droit à l'égard de la même contravention.

Pénalité administrative maximale
(6) La pénalité administrative ne doit pas être supérieure :

a) dans le cas d'une organisation qui est une personne, 50 000 $;
b) dans le cas d'une organisation qui n'est une personne, le plus élevé des montants suivants :
   (i) 10 000 000 $,
   (ii) 3 % du revenu global brut de l'organisation au cours de son exercice précédant celui au cours duquel la pénalité est imposée.

En ce qui concerne le montant maximal des sanctions administratives pécuniaires, l'approche proposée est d'avoir un montant inférieur pour un individu, reflété dans la

partie (a), et de réserver le montant supérieur pour les organisations, tel que reflété dans la partie (b).

> **Prescription de deux ans**
> (7) L'ordonnance exigeant le paiement d'une pénalité administrative ne doit pas être rendue en vertu du présent article plus de deux ans après le jour où la plus récente contravention sur laquelle elle se fonde a été portée à la connaissance du commissaire.

Pour assurer l'équité procédurale, l'Ontario envisage que les ordonnances rendues par le CIPVP, y compris les sanctions administratives pécuniaires, puissent faire l'objet d'un appel devant la Cour divisionnaire sur une question de droit dans un délai de 30 jours.

> **Droit d'appel : ordonnance de conformité**
> (1) Le plaignant ou l'organisation qui est concernée par une ordonnance de conformité peut en interjeter appel devant la Cour divisionnaire sur une question de droit, conformément aux règles de pratique, en déposant un avis d'appel dans les 30 jours qui suivent la réception de l'ordonnance.
>
> **Caractère confidentiel des renseignements**
> (2) Dans le cadre d'un appel interjeté en vertu du présent article, le tribunal peut prendre des précautions afin d'éviter que lui-même ou toute autre personne ne divulgue des renseignements personnels concernant un particulier, notamment, lorsque cela est approprié, la réception d'observations sans préavis, la tenue d'audiences à huis clos ou l'apposition d'un sceau sur les dossiers du greffe.
>
> **Ordonnance du tribunal**
> (4) Lorsqu'il entend un appel en vertu du présent article, le tribunal peut, par ordonnance :
>
> a) enjoindre au commissaire de prendre les décisions et les mesures qu'il est autorisé à prendre en vertu de la présente loi et que le tribunal estime appropriées;
> b) si cela est nécessaire, modifier ou annuler l'ordonnance du commissaire.

Enfin, l'approche proposée par l'Ontario pourrait inclure des infractions statutaires qui tiendraient les organisations responsables de la violation de certaines dispositions importantes de la loi, notamment lorsqu'une organisation omet : de signaler une violation des mesures de sécurité au CIPVP; de tenir un registre de chaque violation des mesures de sécurité; de conserver les renseignements faisant l'objet d'une enquête du CIPVP; de se conformer à une ordonnance de conformité du CIPVP; de réidentifier des renseignements personnels qui ont été dépersonnalisés ou de chercher à se venger d'un dénonciateur.

Infraction
(1) Une organisation est coupable d'une infraction si :

a) elle contrevient sciemment à **[Rapport au commissaire]**, **[Registre]**, **[Interdiction de repersonnaliser les renseignements personnels]**, **[Conservation des renseignements]**, **[Ordonnance de conformité]** ou **[Dénonciation]**;
b) elle entrave le commissaire ou son délégué lorsqu'il examine une plainte, mène une enquête ou procède à une vérification.

Peine
(2) L'organisation qui est coupable d'une infraction prévue au paragraphe (1) est passible, sur déclaration de culpabilité, d'une amende n'excédant pas le plus élevé de 25 000 000 $ et du montant qui correspond à 5 % du revenu global brut de l'organisation au cours de son exercice précédant celui au cours duquel l'organisation est condamnée.

Une autre option pour aider les personnes à obtenir un accès plus rapide aux résolutions est d'inclure des dispositions qui permettraient au CPI d'émettre des décrets aux organisations les obligeant à prendre des mesures pour permettre aux personnes d'être indemnisées en cas d'atteinte à la vie privée. Comme il a été mentionné dans la présentation du CPVP sur le projet de loi C-11, il pourrait s'agir d'un outil utile pour obliger les organisations à offrir de l'aide ou à dédommager les personnes pour les pertes, financières ou autres, en cas de défaillance des mesures de sécurité touchant les renseignements personnels. L'Ontario souhaite recevoir des commentaires sur ce sujet.

Le cadre d'application proposé pourrait soutenir et aider les organisations qui tentent de se conformer à la loi, tout en s'attaquant aux cas flagrants de non-conformité et en dissuadant ainsi les mauvais acteurs. Une surveillance et une application rigoureuses renforceraient la confiance du public dans les plates-formes et les technologies numériques, car les Ontariens pourraient être rassurés en sachant que les mauvais acteurs feraient l'objet d'une enquête et subiraient des conséquences en cas de violation de la loi.

Questions de discussion :

- Les programmes de certification et les codes de pratiques seraient-ils efficaces pour encourager de manière proactive et collaborative les pratiques exemplaires en matière de protection de la vie privée ?
- Les sanctions administratives pécuniaires sont-elles efficaces pour encourager le respect des lois sur la protection de la vie privée ? Les sanctions financières sont-elles fixées à un niveau approprié ?

- La possibilité pour le CIPVP d'émettre des décrets obligeant les organisations à offrir une assistance ou à dédommager les individus serait-elle un outil efficace pour permettre aux individus de résoudre plus rapidement leurs problèmes ?

Soutenir les innovateurs de l'Ontario

Problème :

Les organisations peuvent souhaiter utiliser des renseignements personnels dépersonnalisés à des fins de recherche et d'innovation. Elles peuvent souhaiter améliorer leurs technologies, services ou produits existants ou en développer de nouveaux. De telles utilisations des renseignements dépersonnalisés peuvent améliorer l'activité économique numérique tout en protégeant la vie privée des Ontariens. Pour le faire en toute sécurité, cependant, les organisations doivent être sûres qu'en utilisant des données dépersonnalisées, elles ne contreviennent pas aux règles de protection de la vie privée.

Objectif :

L'Ontario pourrait saisir cette occasion pour énoncer des définitions, des exigences et des normes claires afin de guider les organisations dans l'utilisation des données dépersonnalisées, encourageant ainsi une recherche et une innovation sûres et responsables sans compromettre la vie privée des Ontariens.

*

Avec l'essor des mégadonnées et des techniques d'analyse des données, les organisations et les chercheurs peuvent tirer de nouveaux enseignements des données pour trouver des solutions innovantes à des questions ou des problèmes. Cependant, avec l'accélération de l'analyse des données et de l'IA, il est nécessaire de protéger les individus contre les atteintes potentielles à la vie privée résultant de l'utilisation de grands ensembles de données des renseignements personnels.

Comme indiqué précédemment, l'Ontario envisage d'adopter des règles concernant l'utilisation de systèmes de décision automatisés qui ont un impact important sur les personnes (voir L'utilisation sûre de la prise de décision automatisée). Les restrictions proposées s'alignent sur les travaux menés par l'Ontario pour élaborer un cadre pour une IA digne de confiance. Pour plus d'informations, veuillez consulter la page de consultation sur le Cadre de l'intelligence artificielle (IA) de confiance de l'Ontario. En outre, l'Ontario envisage un cadre qui encouragerait et, dans certains cas, obligerait les organisations à utiliser des renseignements dépersonnalisés, dans la mesure du possible, afin de réduire les risques de préjudice pour la personne, tout en clarifiant les obligations des organisations à l'égard des renseignements dépersonnalisés.

« renseignements dépersonnalisés » : information sur une personne qui ne permet plus d'identifier directement ou indirectement la personne sans utiliser d'autres informations.

La confusion règne souvent quant à la place des renseignements dépersonnalisés dans les lois sur la protection de la vie privée, car ces dernières ne régissent généralement que les « renseignements personnels » et sont muettes sur le sujet des renseignements dépersonnalisés. De nos jours, les renseignements dépersonnalisés ont été transformés de telle manière qu'ils ne sont plus identifiables, ce qui semblerait indiquer qu'ils ne sont plus soumis aux règles de protection de la vie privée; cependant, ils sont dérivés des renseignements personnels et certains risques de préjudice pour les personnes peuvent encore exister, notamment le potentiel de réidentification.

Pour cette raison, l'Ontario envisage une approche qui étendrait certaines exigences aux renseignements dépersonnalisés. Il pourrait s'agir d'exigences liées à la mise en œuvre d'un programme de gestion de la vie privée, à la mise en place de mesures de sécurité pour protéger les renseignements dépersonnalisés et à la possibilité de déposer une plainte ou de demander des renseignements sur la conformité.

L'objectif de cette approche proposée est de faire en sorte que les organisations soient transparentes et responsables de l'utilisation qu'elles font des renseignements dépersonnalisés. Elle reconnaîtrait également que certaines caractéristiques d'un cadre de protection de la vie privée ne sont ni souhaitables ni réalisables lorsqu'il s'agit de renseignements personnels dépersonnalisés. Par exemple, si les renseignements ont été dépersonnalisés, les organisations ne seraient pas tenues de répondre à une demande d'accès, d'ajout, de transfert ou de suppression de renseignements personnels présentée par une personne.

L'Ontario envisage un cadre de dépersonnalisation fondé sur une approche axée sur le risque, qui obligerait les organisations à utiliser des protocoles de dépersonnalisation proportionnels à la sensibilité des renseignements personnels. L'Ontario envisage également d'interdire la réidentification des renseignements personnels, sauf en conformité avec les mesures techniques et administratives stipulées, y compris les mesures de protection de la vie privée.

Proportionnalité des procédés techniques et administratifs
Lorsque l'organisation dépersonnalise des renseignements personnels, elle veille à ce que les procédés techniques et administratifs utilisés soient proportionnels aux fins auxquelles ces renseignements sont dépersonnalisés et au caractère délicat des renseignements personnels.

> **Interdiction**
> Sauf si la loi l'exige et sous réserve des exceptions et des exigences supplémentaires prescrites, il est interdit à toute personne ou organisation d'utiliser ou de tenter d'utiliser des renseignements dépersonnalisés, seuls ou en combinaison avec d'autres renseignements, afin d'identifier un individu à des fins autres que la vérification de l'efficacité des mesures de sécurité qu'elle a mises en place pour protéger les renseignements, sauf si cela est fait conformément aux protocoles techniques et administratifs indiqués incluant la protection de la vie privée des particuliers.

Ces recommandations reflètent celles que la commissaire à l'information et à la protection de la vie privée de l'Ontario a formulées dans ses observations lors de la consultation de 2020 sur la réforme de la protection de la vie privée. Le CIPVP est un acteur de premier plan en matière d'anonymisation; il a publié en 2016 des lignes directrices reconnues sur l'anonymisation des données structurées intitulées De-Identification Guidelines for Structured Data.

Enfin, le concept de « données anonymes » - des renseignements personnels qui ont été modifiés de telle manière qu'ils ne sont plus identifiables par rapport à une personne - est également envisagé. Ce concept élargirait encore les approches de l'utilisation des données fondées sur le risque et encouragerait l'utilisation de données anonymes en les retirant complètement des règles de protection de la vie privée.

> **Renseignements anonymisés**
> (3) Pour plus de clarté, la présente loi ne s'applique pas aux renseignements qui ont été modifiés de façon irréversible, selon les pratiques exemplaires généralement acceptées, de telle sorte qu'aucun individu ne puisse être identifié à partir des renseignements, que ce soit directement ou indirectement par quelque moyen ou par quelque personne que ce soit.

L'approche proposée pour les renseignements dépersonnalisés pourrait promouvoir l'innovation par l'analyse des données, tout en protégeant la vie privée. Les organisations seraient incitées à gérer les risques d'atteinte à la vie privée en utilisant des techniques de dépersonnalisation et d'anonymisation lorsqu'elles effectuent des analyses. Ces techniques pourraient contribuer à réduire les risques résiduels de préjudice pour les personnes sans empêcher les organisations de réaliser la valeur des données.

L'utilisation responsable des renseignements dépersonnalisés peut grandement contribuer au bien public. Par conséquent, les exigences proposées pourraient aider à jeter les bases permettant à l'Ontario d'explorer des modèles d'intendance et de gouvernance des données, ainsi que des systèmes de partage sécuritaire de l'information qui pourraient faire progresser la collecte, l'utilisation et la divulgation des

données à des fins socialement bénéfiques. Le gouvernement examine attentivement ces options et accueillera les commentaires des Ontariens pour éclairer cette prochaine phase importante du travail politique, alors que la province continue de mettre en œuvre sa Stratégie pour le numérique et les données et d'explorer les autorités en matière de données pour fournir un accès sûr et partagé à l'information. Bien que le monde numérique présente des risques, un régime plus protecteur de la vie privée peut aider à débloquer de nouveaux avantages et des innovations pour l'avenir de la province.

Questions de discussion :

- L'articulation plus claire des règles de protection de la vie privée qui s'appliquent aux renseignements dépersonnalisés, comme discuté dans cette section, encouragerait-elle les organisations à utiliser des renseignements dépersonnalisés, et donc à réduire le risque d'atteinte à la vie privée ?
- L'inclusion du concept de renseignements dépersonnalisés, et la clarification du fait que la loi sur la protection de la vie privée ne s'appliquerait pas à cette information, encourageraient-elles les organisations à utiliser des renseignements dépersonnalisés ?
- Dans le cas du partage d'informations à des fins d'utilité sociale, quelles mesures de protection ou de gouvernance supplémentaires seraient nécessaires, en plus de la dépersonnalisation des renseignements, afin de protéger la vie privée ?

3 Conclusion

La confiance du public dans l'économie numérique est essentielle à la prospérité future de l'Ontario et au bien-être des Ontariens. L'approche proposée par l'Ontario en jetterait les bases en mettant en œuvre une approche de la protection de la vie privée fondée sur les droits afin d'habiliter les Ontariens et de donner aux organisations ontariennes un avantage concurrentiel dans un monde axé sur les données.

Alors que de nombreuses organisations en Ontario observent déjà une norme élevée de protection de la vie privée dans leurs activités, d'autres peuvent être confrontées à certains défis lorsqu'elles adaptent leurs pratiques et leurs services aux nouvelles exigences. Les changements réglementaires peuvent être difficiles, et la protection des données a besoin de temps pour s'améliorer. L'Ontario reconnaît que l'approche proposée dans le présent document nécessiterait une période de transition et envisage un minimum de deux ans, si une loi est présentée, pour que la loi entre en vigueur. Si une loi sur la protection de la vie privée est présentée et adoptée, l'Ontario envisagerait de prévoir un minimum de deux ans avant l'entrée en vigueur des règles.

L’approche proposée exigerait une mise en œuvre séquentielle, la fourniture de ressources - notamment sous la forme de documents d’orientation conviviaux, de programmes de certification et de codes de pratique pour familiariser les organisations avec les nouvelles obligations - et l’établissement de normes cohérentes et interopérables. La province continuerait également à faire appel à des intervenants de différents secteurs pour obtenir des commentaires sur l’orientation et la mise en œuvre afin de s’assurer que leurs secteurs sont soutenus de façon appropriée pendant la transition.

En tant que chef de file en matière de protection des données, l’Ontario pourrait également devenir l’une des principaux territoires numériques au monde - et établir une base de protection de la vie privée qui habilitera les Ontariens, protégera leurs renseignements personnels et favorisera l’innovation responsable et l’utilisation des données pour le bien public.

COMMENT PARTICIPER

Réponse formelle

Nous vous invitons à nous faire part de vos commentaires sur les détails et les projets de dispositions présentés dans ce document. Si vous êtes une organisation, un expert juridique ou technique, ou un membre du public et que vous souhaitez soumettre une réponse officielle à ce document, vous pouvez le faire à l’adresse suivante : access.privacy@ontario.ca.

Votre vie privée compte

Nous vous demandons de nous faire part de vos commentaires afin de nous aider à comprendre les préoccupations des Ontariens en matière de protection de la vie privée et à trouver la meilleure façon de répondre à ces préoccupations par le biais de politiques, de lois ou de règlements.

Ces commentaires seront utilisés par le ministère des Services gouvernementaux et des Services aux consommateurs pour nous aider à élaborer un cadre de protection de la vie privée en Ontario qui réponde à vos besoins.

Si vous fournissez votre adresse électronique, elle ne sera pas associée à vos commentaires et ne sera utilisée que pour vous tenir au courant de cette initiative et vous informer des consultations futures. Votre adresse électronique ne sera pas placée sur des listes de diffusion ni communiquée à des tiers, sauf dans les cas où la loi l’autorise.

Pour toute question sur l’utilisation des informations recueillies sur cette page, veuillez nous contacter :

Chef, Unité des stratégies et des politiques relatives à l’accès à l’information et à la protection de la vie privée
Ministère des Services gouvernementaux et des Services aux consommateurs
Direction de la conservation des documents, de l’accès à l’information et de la protection de la vie privée pour la FPO
134, boulevard Ian Macdonald
Toronto (Ontario)
M7A 2C5
Téléphone : 416-327-1600 ou 1-800-668-9933 (numéro sans frais - Ontario seulement)