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

Le 24 juin 2024 ***PAR COURRIER ÉLECTRONIQUE ET EN LIGNE***

Madame Meghan Stenson
Greffière des services de la procédure
Direction des services de la procédure
Édifice Whitney
Pièce 1405
99, rue Wellesley Ouest
Toronto ON M7A 1A2

Objet : Mémoire sur le projet de loi 194, *Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public*

Madame,

La présente a trait au projet de loi 194, *Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public*, qui est actuellement en deuxième lecture à l'Assemblée législative de l'Ontario. Les travaux de l'Assemblée étant suspendus, je vous remets le mémoire de mon bureau à l'intention du comité qui sera chargé d'étudier le projet de loi 194 après le retour des députés, le 21 octobre 2024.

Le projet de loi 194 est un texte législatif fondamental. S'il était adopté, son annexe 1 établirait des exigences concernant la cybersécurité et les systèmes d'intelligence artificielle (IA) pour les entités du secteur public, ainsi que des règles sur l'utilisation des technologies numériques touchant les enfants et les jeunes de moins de 18 ans. L'annexe 2 modifie la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) en instaurant de nouvelles mesures de protection de la vie privée et en renforçant la surveillance.

En tant que commissaire à l'information et à la protection de la vie privée de l'Ontario, je suis une haute fonctionnaire indépendante de l'Assemblée législative dont le mandat consiste à protéger les droits des particuliers en matière d'accès à l'information et de protection de la vie privée. Je félicite le gouvernement de chercher à répondre aux besoins actuels des Ontariennes et des Ontariens, en particulier les enfants et les jeunes, qui sont confrontés à des menaces constantes en matière de cybersécurité et à l'utilisation croissante de l'IA et qui sont exposés à de graves risques et préjudices pour leur vie privée en ligne.

Ce projet de loi se concentre à juste titre sur les aspects fondamentaux qui influent sur le bien-être de la population ontarienne dans un monde de plus en plus numérisé. Il s'aligne sur d'autres réformes législatives mondiales visant à réagir aux progrès technologiques rapides et à leurs incidences sociales plus larges. Nous nous trouvons à un moment critique, à la croisée des chemins entre risques et possibilités, où les décisions que nous prenons aujourd'hui façonneront indéniablement notre avenir pour les générations à venir.

Le CIPVP s'efforce de faire en sorte que les droits en matière de protection de la vie privée et d'accès à l'information des Ontariennes et des Ontariens soient pris en compte et respectés à ce tournant décisif. Nous avons pour but de préparer la population ontarienne à son avenir numérique et, en collaboration avec nos homologues fédéraux, provinciaux et territoriaux, nous réclamons des mesures de précaution plus solides et une transparence accrue. Conscients de

l'essor de l'IA, nous avons collaboré, sur la scène nationale et internationale, à l'élaboration de résolutions, de prises de position et de recommandations de réformes législatives liées à l'IA dans les domaines des politiques publiques, de la santé et de l'emploi.

Il n'a jamais été aussi important de moderniser les lois ontariennes sur l'accès à l'information et la protection de la vie privée. Il est indispensable de disposer de lois modernes et efficaces pour renforcer la reddition de comptes, la transparence et la surveillance nécessaires pour protéger les droits et tirer profit des occasions qui se présentent dans un monde en évolution rapide. Dans le présent mémoire, je propose plusieurs recommandations visant à renforcer le projet de loi 194 et à combler les lacunes importantes qu'il présente sous sa forme actuelle. Ces recommandations s'articulent autour de trois grands thèmes :

1. Adopter une approche fondée sur des principes pour régir les nouveaux domaines d'activité à risque élevé, comme l'intelligence artificielle, qui influent sur la façon dont les Ontariennes et les Ontariens vivent, travaillent et interagissent avec les institutions publiques. Ces principes devraient être inscrits expressément dans la loi et refléter notre engagement collectif en faveur des droits fondamentaux et des valeurs communes qui sous-tendent notre société libre et démocratique. Ces principes devraient encadrer l'élaboration et l'utilisation des nouvelles technologies, en veillant à ce qu'elles profitent à la société et favorisent l'épanouissement de l'être humain.

2. Veiller à ce que le gouvernement soit plus transparent quant à la manière dont il propose de réglementer la cybersécurité, l'intelligence artificielle et les technologies numériques accessibles aux enfants et aux jeunes de moins de 18 ans. En procédant à des consultations publiques et en faisant preuve de plus d'ouverture et de transparence dans son processus de réglementation, le gouvernement peut élaborer des règlements plus efficaces, adaptés aux besoins et aux réalités des différents groupes et communautés. En définitive, les institutions publiques disposeraient ainsi de règles claires, concrètes et prévisibles qu'elles pourraient mieux comprendre et appliquer dans la pratique, et dans le cadre desquelles elles pourraient innover de manière plus sûre et plus responsable.

3. Renforcer la responsabilisation et la surveillance indépendante des entités du secteur public afin de garantir le respect des nouvelles règles proposées. Il s'agit notamment de veiller à ce que tout Ontarien ou Ontarienne qui croit raisonnablement que sa vie privée et ses droits ont été violés dispose d'un recours et à protéger les dénonciateurs contre les représailles. Un système de surveillance et d'application cohérent, rationalisé et indépendant du gouvernement renforcera la confiance dans les institutions publiques qui utilisent les technologies de manière responsable et garantira la prospérité économique et sociale de toute la population ontarienne.

ANNEXE 1 DU PROJET DE LOI 194 :
LOI DE 2024 VISANT À RENFORCER LA SÉCURITÉ ET LA CONFIANCE EN MATIÈRE DE NUMÉRIQUE

Dans sa version actuelle, cette loi établirait des pouvoirs réglementaires importants en matière de cybersécurité, de systèmes d'intelligence artificielle et de technologies numériques touchant les personnes de moins de 18 ans. Le CIPVP convient que ces domaines d'activité sociale présentent un risque élevé pour le droit à la vie privée et les autres droits des Ontariens et des Ontariennes, et qu'ils nécessitent une intervention urgente de la part du gouvernement. Cependant, dans son libellé actuel, l'annexe 1 du projet de loi 194 ne prévoit pas de mesures de protection du droit à la vie privée et des autres droits de la personne, ni le niveau de transparence et de reddition de comptes nécessaire pour que la population de l'Ontario puisse avoir confiance dans la manière dont le gouvernement régira ces activités à risque élevé.

Les recommandations suivantes visent à promouvoir les objectifs sous-jacents de l'annexe 1 en donnant aux Ontariennes et aux Ontariens la certitude que leur droit à la vie privée et leurs autres droits sont importants, que des principes clairs et transparents régissent les décisions et les activités des institutions et qu'un système de surveillance efficace garantit leur bonne application.

A. Recommandations générales concernant l'annexe 1

L'annexe 1 devrait comprendre une disposition d'objet

La *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* proposée ne contient pas de règles de fond sur la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels dans le contexte des incidents de cybersécurité, des systèmes d'IA ou des technologies touchant les enfants et les jeunes. Elle n'indique pas expressément comment ces renseignements personnels seront protégés et surveillés de manière indépendante, et n'offre pas le niveau de transparence que la population ontarienne attend et mérite de la part de ses institutions publiques.

Dans son préambule, la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* reconnaît « l'importance de protéger la vie privée de la population de l'Ontario et d'améliorer les mesures de précaution déployées à cet égard grâce à une transparence accrue et un système de surveillance indépendant ». Or, un préambule à lui seul n'a pas force de loi. Il ne confère pas de droits fondamentaux individuels ou collectifs, ni ne définit les fonctions et obligations d'une organisation publique en vue de protéger ces droits. De plus, les tribunaux n'interprètent pas toujours les préambules de la même façon, ce qui rend le texte de loi encore moins clair et prévisible pour les institutions et le public.

Par contre, une disposition d'objet permet de mieux expliquer comment la loi sera interprétée et d'établir des balises plus claires afin de protéger le droit à la vie privée et les autres droits des Ontariennes et des Ontariens[1]. Le CIPVP recommande d'ajouter à la loi une disposition d'objet

[1] Dans ses observations sur le projet de loi 194, la professeure Teresa Scassa recommande également au gouvernement d'intégrer une disposition d'objet dans la loi et de l'assortir de principes clairement définis afin d'orienter l'adoption et l'utilisation de l'IA dans le secteur parapublic : [traduction] « Cette partie a pour objet de faire en sorte que les systèmes d'intelligence artificielle qu'adoptent et utilisent les entités du secteur public soient élaborés, adoptés, utilisés et tenus à jour d'une manière transparente et responsable qui respecte le droit à la vie privée et les autres droits des Ontariennes et des Ontariens ».

qui rendrait plus explicite l'intention du gouvernement et formulerait des principes directeurs clairs sur l'interprétation et l'application de la loi.

Recommandation 1 : Amender l'annexe 1 par adjonction de cette disposition d'objet :

> ***[X] La présente loi a pour objet d'établir un cadre de gouvernance pour les entités du secteur public concernant les activités de cybersécurité, l'utilisation de systèmes d'intelligence artificielle et le déploiement de technologies numériques touchant les particuliers de moins de 18 ans, conformément aux principes suivants :***
>
> ***a) la vie privée des particuliers et des groupes doit être protégée, et il doit être interdit de recueillir, d'utiliser, de conserver et de divulguer plus de leurs renseignements personnels qu'il n'est nécessaire et proportionné pour réaliser la fin visée;***
> ***b) les entités du secteur public doivent remplir leurs obligations en vertu de la présente loi avec transparence dans la mesure où il est raisonnable et approprié de le faire, sans porter atteinte à la sécurité et à l'intégrité des systèmes d'information du gouvernement;***
> ***c) les systèmes d'intelligence artificielle doivent être valides, fiables et sûrs; ils doivent être conçus pour protéger la vie privée et affirmer les droits de la personne, et les entités du secteur public qui les utilisent doivent être responsables et transparentes;***
> ***d) les normes relatives aux technologies numériques touchant les personnes de moins de 18 ans doivent être élaborées et appliquées en tenant compte des droits des enfants et des jeunes et être conformes aux valeurs que sont l'autonomie personnelle, la dignité et l'autodétermination;***
> ***e) l'observation des dispositions de la présente loi et des règlements devrait être surveillée de façon indépendante du gouvernement.***

La loi devrait être assujettie à une surveillance et à une application indépendantes

En vertu de l'annexe 1, le gouvernement réglementerait une série de technologies numériques qui comportent la collecte, l'utilisation, la conservation et la divulgation de renseignements personnels concernant les Ontariennes et les Ontariens, ce qui relève directement du champ de compétence du CIPVP. Elle confère exclusivement au gouvernement la responsabilité de surveiller l'observation par le secteur public de règles et de directives qui restent à établir, sans aucune disposition d'application et sans aucune conséquence en cas d'inobservation. Ce modèle d'autogestion ne représente pas ce à quoi la population ontarienne pourrait raisonnablement attendre pour réglementer ces domaines d'activité à risque élevé qui ont une incidence sur les droits fondamentaux. Comme pour d'autres activités du secteur public dont les répercussions sur la vie des Ontariennes et des Ontariens sont aussi directes et importantes, la surveillance et l'application des lois doivent être assurées de manière indépendante du gouvernement.

Nous recommandons donc que l'annexe 1 soit modifiée afin d'inclure une disposition faisant expressément référence au rôle indépendant de surveillance et d'application de la loi du CIPVP,

qui est maintenu en ce qui concerne les droits en matière de protection de la vie privée et d'accès à l'information sur lesquels pourraient influer les types de programmes de cybersécurité, d'IA et de technologie numérique envisagés par la loi.

Recommandation 2 : Amender l'annexe 1 afin de reconnaître expressément le rôle et les fonctions du CIPVP en tant qu'organisme de surveillance indépendant par adjonction de la disposition suivante :

> ***[X] Le commissaire à l'information et à la protection de la vie privée exerce les fonctions et pouvoirs attribués par la*** **Loi sur l'accès à l'information et la protection de la vie privée,** ***la*** **Loi sur l'accès à l'information municipale et la protection de la vie privée,** ***la*** **Loi de 2004 sur la protection des renseignements personnels sur la santé,** ***la*** **Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille** ***et tout autre texte de loi qui lui attribue des pouvoirs et fonctions relativement aux entités du secteur public qui sont assujetties à la présente loi.***

Les règlements pris en vertu de la loi devraient faire l'objet de consultations publiques

D'importantes parties de la législation proposée seront adoptées par règlement. Il s'agit notamment de règles de fond, fondées sur des valeurs, destinées à régir le déploiement et l'adoption de systèmes d'IA et de technologies numériques mises à la disposition des enfants et des jeunes. Pour les raisons exposées ci-dessous, nous sommes convaincus que ces règles et principes d'ordre supérieur, qui reflètent des valeurs sociales importantes, devraient être codifiés dans la loi elle-même. Si le gouvernement souhaite tout de même prendre des règlements pour préciser des règles et des exigences plus techniques, ces règlements devraient à tout le moins être transparents et faire l'objet d'une consultation publique.

En outre, le ministre devrait être tenu de prendre en compte les opinions et les commentaires des Ontariennes et des Ontariens, en particulier ceux de populations ou de groupes défavorisés ou marginalisés qui tendent à être écartés du processus de réglementation. L'obligation expresse de tenir des consultations publiques avant de prendre des règlements et de tenir compte de la diversité des points de vue des Ontariennes et des Ontariens pourrait s'inspirer de dispositions semblables qui existent dans les lois actuelles, telles que l'article 74 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS). Nous recommandons donc qu'un mécanisme de consultation publique obligatoire soit inclus dans l'annexe 1 du projet de loi 194 afin que le ministre tienne compte des opinions et des commentaires des Ontariennes et des Ontariens avant de prendre des règlements sur des questions aussi importantes qui ont une incidence sur leurs droits fondamentaux.

Recommandation 3 : Amender l'annexe 1 pour prescrire un processus de consultation publique préalable à la prise de règlements en application de la loi. Cette exigence devrait s'inspirer de l'article 74 de la LPRPS.

Le ministre devrait consulter le CIPVP avant de prendre (ou de proposer) des règlements ou de donner des directives qui pourraient se répercuter sur les droits en matière de protection de la vie privée et d'accès à l'information

L'annexe 1 permet au gouvernement de prendre des règlements (directement ou par l'intermédiaire du lieutenant-gouverneur en conseil) et de donner des directives concernant les programmes de cybersécurité, l'utilisation de systèmes d'IA et le déploiement de technologies numériques touchant les particuliers de moins de 18 ans. Ces règlements et directives feront inévitablement double emploi avec les règles existantes applicables aux documents et renseignements personnels dont des entités du secteur public ont la garde ou le contrôle en vertu des lois ontariennes sur l'accès à l'information et la protection de la vie privée, qui sont soumises à la surveillance du CIPVP. Ainsi, les entités du secteur public pourraient devoir composer avec des règles et des directives faisant éventuellement double emploi, voire divergentes.

L'article 14 de l'annexe 1 propose de résoudre toute incompatibilité de la façon suivante : « Les dispositions de toute autre loi ou règlement l'emportent sur les dispositions incompatibles de la présente loi ou des règlements pris ou des directives données en vertu de la présente loi. » Cependant, nous pensons qu'il faudrait faire plus pour réduire le risque de règles contradictoires. L'objectif devrait être d'éviter les doubles emplois et de minimiser le risque de confusion et d'incohérence pour les entités du secteur public, qui pourrait conduire à une inobservation involontaire et éventuellement aller à l'encontre des objectifs du projet de loi.

Nous recommandons que l'annexe 1 soit amendée pour exiger que le ministre consulte le CIPVP avant de prendre ou de proposer des règlements ou de donner des directives susceptibles d'avoir une incidence sur les droits en matière d'accès à l'information ou de protection de la vie privée. Un tel amendement serait semblable aux dispositions actuelles d'autres lois ontariennes prévoyant une telle consultation obligatoire du CIPVP et aurait pour avantage d'assujettir les entités du secteur public à des règles et directives uniformes. (Voir par exemple les paragraphes 55.4 (2) et (3) de la LPRPS, qui pourraient être adaptés à cette fin.)

Recommandation 4 : Amender l'annexe 1 afin que le ministre soit tenu de consulter le CIPVP avant de proposer ou de prendre un règlement ou de donner une directive pouvait se répercuter sur les droits des Ontariennes et Ontariens en matière d'accès à l'information et de protection de la vie privée. Cet amendement devrait s'inspirer des paragraphes 55.4 (2) et (3) de la LPRPS.

Les directives ministérielles devraient être transparentes pour le public

Un objectif essentiel de l'annexe 1 est de renforcer la confiance du public dans la manière dont les entités du secteur public sécurisent leurs systèmes d'information contre les risques liés à la cybersécurité et déploient des technologies numériques touchant les enfants et les jeunes. Pour instaurer la confiance, il est essentiel d'assurer la transparence des directives que donne le ministre, afin que les Ontariennes et les Ontariens puissent comprendre les caractéristiques générales du cadre réglementaire et avoir confiance en son efficacité.

Une transparence accrue peut également avoir pour effet positif de sensibiliser et de mobiliser davantage le grand public, qui pourrait alors mieux comprendre la nature des risques encourus, poser des questions plus éclairées aux institutions publiques avec lesquelles il est en contact, et

participer en connaissance de cause à ses propres efforts de sensibilisation au numérique et de protection de ses renseignements personnels en ligne.

Dans son libellé actuel, la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* soustrait les directives ministérielles à la partie III de la *Loi de 2006 sur la législation*, y compris l'obligation de publier les directives dans le site Web Lois-en-ligne et dans la *Gazette de l'Ontario*. L'annexe 1 n'exige pas que le gouvernement publie les directives ministérielles que les entités du secteur public doivent observer. Nous recommandons donc que l'annexe 1 soit amendée pour exiger que ces directives soient rendues publiques afin que les Ontariennes et Ontariens puissent mieux comprendre les mesures que les entités du secteur public sont tenues de prendre et s'assurer qu'elles les prennent.

Recommandation 5 : Amender l'annexe 1 pour exiger que les directives du ministre soient promulguées publiquement. Plus précisément, amender l'annexe 1 par adjonction des dispositions suivantes après les paragraphes 4 (3) et 11 (3) :

4 (X) Chaque directive donnée en vertu du paragraphe 4 (1) de la présente loi, à la fois :

- ***a) est mise à la disposition du public, sur demande;***
- ***b) est affichée publiquement sur au moins un site Web du gouvernement de l'Ontario.***

11 (X) Chaque directive donnée en vertu du paragraphe 11 (1) de la présente loi, à la fois :

- ***a) est mise à la disposition du public, sur demande;***
- ***b) est affichée publiquement sur au moins un site Web du gouvernement de l'Ontario.***

L'annexe 1 devrait comprendre une disposition sur la dénonciation

Un régime d'observation visant à réglementer des activités à risque élevé, telles que celles proposées par l'annexe 1 du projet de loi 194, est parfois tributaire des actes courageux de personnes travaillant au sein d'entités du secteur public, qui communiquent des renseignements ou des allégations concernant des erreurs ou des omissions de leurs collègues ou supérieurs. Afin que les employés se sentent assez en sécurité pour communiquer des renseignements importants pour préserver l'intégrité du régime d'observation, y compris les exigences prescrites en matière de rapports, ils doivent avoir l'assurance que la confidentialité sera respectée et qu'il n'y aura pas de représailles. Nous recommandons donc que l'annexe 1 soit amendée pour prévoir expressément des mesures de protection des dénonciateurs.

Bien que l'article 10 de l'annexe 2 du projet de loi 194 contienne une disposition relative aux dénonciateurs, celle-ci ne s'appliquerait qu'aux institutions provinciales et uniquement en ce qui concerne les infractions présumées à la LAIPVP et à ses règlements. L'article 10 de l'annexe 2 ne s'appliquerait pas à toutes les autres entités du secteur public, y compris les institutions régies par la LAIMPVP, les sociétés d'aide à l'enfance ou les conseils scolaires, ni aux contraventions présumées à l'annexe 1 ou à ses règlements.

Recommandation 6 : Amender l'annexe 1 pour protéger expressément les dénonciateurs.

Dénonciation
[X] (1) Quiconque a des motifs raisonnables de croire qu'une entité du secteur public ou toute autre personne a contrevenu à la présente loi, aux règlements ou à une directive aux termes de la présente loi ou est sur le point de le faire peut en aviser le commissaire ou un fonctionnaire désigné par le ministre et demander que son identité soit gardée confidentielle relativement à cette dénonciation.

Caractère confidentiel
(2) Le commissaire ou le fonctionnaire désigné par le ministre est tenu de garder confidentielle l'identité de la personne qui l'a avisé en vertu du paragraphe (1) et à laquelle il a donné l'assurance de l'anonymat.

Représailles interdites
(3) Nul ne doit congédier, suspendre, rétrograder, punir ou harceler une personne ou lui faire subir tout autre désavantage pour l'un des motifs suivants :

- ***a) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a divulgué au commissaire qu'une autre personne a contrevenu à une disposition de la présente loi ou des règlements ou à une directive ou est sur le point de faire;***
- ***b) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a accompli ou fait part de son intention d'accomplir tout acte nécessaire pour empêcher une personne de contrevenir à une disposition de la présente loi ou des règlements ou à une directive;***
- ***c) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a refusé d'accomplir ou fait part de son intention de refuser d'accomplir tout acte qui est en contravention à une disposition de la présente loi ou des règlements ou à une directive;***
- ***d) quelqu'un croit que la personne accomplira un des actes visés à l'alinéa a), b) ou c).***

Peine
(4) La personne qui enfreint le paragraphe (3) est coupable d'une infraction et est passible, sur déclaration de culpabilité, d'une amende d'au plus 5 000 $.

B. Recommandations portant sur la partie de l'annexe 1 qui concerne la cybersécurité

Les entités du secteur public sont de plus en plus touchées par une forte hausse des incidents liés à la cybersécurité, y compris des attaques par rançongiciel. Selon le Centre canadien pour la cybersécurité, des individus malveillants s'en prennent de plus en plus à des infrastructures essentielles et à des services publics[2]. Les municipalités, les universités, les écoles et les

[2] Centre canadien pour la cybersécurité (2022). *Évaluation des cybermenaces nationales 2023-2024*. Disponible à : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024.

hôpitaux sont particulièrement exposés aux cybercrimes, ce qui représente une grave menace pour les renseignements personnels les plus délicats des Ontariennes et des Ontariens[3] et risque de perturber des services publics essentiels ou d'importance vitale[4], et il faut consacrer des millions de dollars en fonds publics pour rétablir ces services[5], parfois avec un succès mitigé[6].

Les gouvernements agissent rapidement pour améliorer la gouvernance des institutions publiques en matière de cybersécurité et les protections dont bénéficient les citoyens[7]. Le CIPVP appuie l'intention du gouvernement de mettre en place un régime de gouvernance de la cybersécurité pour la population ontarienne. Cependant, nous estimons qu'il est possible d'améliorer l'annexe 1 à plusieurs égards, notamment en ce qui concerne les incidents liés à la cybersécurité qui font intervenir des renseignements personnels.

Les principaux éléments d'un programme de cybersécurité devraient être énumérés expressément dans la loi

La protection des renseignements personnels des Ontariennes et des Ontariens nécessite des programmes de cybersécurité solides et robustes. Bien que ces programmes puissent présenter des particularités propres à chaque institution, tous devraient comporter des éléments de base communs. Par exemple, la partie 2 du projet de loi C-26 du gouvernement fédéral, la *Loi sur la protection des cybersystèmes essentiels*, énumère une série d'éléments de base que les entités concernées doivent inclure dans les programmes de cybersécurité que prescrit la loi, précisant que ces éléments pourraient être élargis par voie de règlement. Ces éléments

---

[3] Autorité canadienne pour les enregistrements Internet (2023). « Pourquoi les municipalités, les écoles, les hôpitaux et les universités sont-ils toujours les plus grandes cibles des cybercriminel·les? ». Disponible à : https://www.cira.ca/fr/ressources/nouvelles/cybersecurite/pourquoi-les-municipalites-les-ecoles-les-hopitaux-et-les-universites-sont-ils-toujours-les-plus-grandes-cibles-des-cybercriminels/.

[4] Jacquelyn LeBel (2024). « More than 325K patient files stolen in cyberattack on 5 southwestern Ontario hospitals », *Global News.* Disponible à : https://globalnews.ca/news/10399865/patient-files-stolen-cyberattack-southwestern-ontario-hospitals/. Kevin Lamb (2024). « Area medical clinics partially crippled by 'cyber-security incident' », *Orillia Matters*. Disponible à : https://www.orilliamatters.com/police-beat/area-medical-clinics-partially-crippled-by-cyber-security-incident-8438750. Hannah Neprash et coll. (2023). « We tried to quantify how harmful hospital ransomware attacks are for patients. Here's what we found », *Stat*. Disponible à : https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/.

[5] Le coût moyen engagé par les organisations canadiennes en cas d'attaque par rançongiciel s'est élevé à plus de 1,1 million de dollars canadiens en 2023. Voir Nathanial Dove (2023). « Canadian firms paying 'significantly' more in ransomware attacks: data », *Global News*. Disponible à : https://globalnews.ca/news/10155151/companies-1-million-ransomware-attacks/.

[6] L'étude canadienne sur les rançongiciels menée par TELUS en 2022 a révélé que 15 % des organisations canadiennes qui avaient subi une attaque par rançongiciel ont été réinfectées par le même rançongiciel après leur rétablissement.

[7] Voir par exemple : Gouvernement du Canada (2024). « Stratégie intégrée de cybersécurité du gouvernement du Canada ». Disponible à : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/strategie-integree-cybersecurite.html. White House (2021). « Executive Order on Improving the Nation's Cybersecurity ». Disponible à : https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. United Kingdom Cabinet Office (2022). « Government Cyber Security Strategy: 2022 to 2030 ». Disponible à : https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

représentent des pratiques exemplaires établies par un éventail d'organismes fédéraux, y compris Sécurité publique Canada.

Nous recommandons que l'annexe 1 du projet de loi 194, à l'instar du projet de loi fédéral C-26, prévoie la prise de règlements sur les éléments de base que doit comporter un programme de cybersécurité, et que ces éléments correspondent à ceux qui sont exigés au palier fédéral. Sachant que les entités du secteur public pourraient avoir besoin de temps pour mettre en place ces programmes de cybersécurité, le gouvernement pourrait également envisager de modifier la loi afin de prévoir une date d'entrée en vigueur ou un délai précis pour la mise en place de ces programmes.

Recommandation 7 : Amender le paragraphe 2 (2) de l'annexe 1 afin que tout règlement sur les programmes de cybersécurité des entités du secteur public prévoie que tous les programmes comprennent certains éléments de base.

> *Règlements : programmes*
>
> *(2) Sans préjudice de la portée générale de l'alinéa (1) b), un règlement pris en vertu de cet alinéa ~~peut~~ exige~~r~~ que le programme d'une entité du secteur public comprenne ce qui suit :*
>
> > *[…]*
> >
> > ***f) l'identification et la gestion de tout risque lié à la cybersécurité pour l'organisation, y compris les risques associés à la chaîne d'approvisionnement de l'entité du secteur public et à son recours à des produits et services externes;***
> > ***g) des mesures visant à protéger contre toute attaque les systèmes informatiques de l'entité;***
> > ***h) des processus visant à déceler les incidents liés à la cybersécurité qui portent ou peuvent porter atteinte aux systèmes informatiques d'une entité du secteur public;***
> > ***i) des procédures visant à minimiser les répercussions des incidents liés à la cybersécurité.***

Le CIPVP devrait être informé des incidents liés à la cybersécurité faisant intervenir des renseignements personnels

Une grande partie du contenu du régime de cybersécurité proposé à l'annexe 1 sera établie plus tard par règlement. L'une des exigences à définir par règlement prévoit que les entités du secteur public devront soumettre au ministre (ou à une personne désignée) des rapports sur les incidents liés à la cybersécurité. Le contenu de ces rapports peut varier en fonction des différents types d'incidents. De manière générale, le CIPVP est favorable à cette obligation de faire rapport qui aidera le ministre à déterminer la nature, le nombre et la gravité des incidents qui touchent les entités du secteur public, à évaluer l'évolution des cybermenaces et à prendre des décisions éclairées en matière d'affectation des ressources pour faire face à ces menaces ou les atténuer.

Les incidents liés à la cybersécurité qui sont signalés au ministre peuvent faire intervenir des renseignements personnels concernant des Ontariennes et des Ontariens. Or, le CIPVP pourrait ne pas être alerté si l'entité déclarante sous-estime le risque que des renseignements personnels aient pu être en cause. Nous recommandons donc que le ministre informe le CIPVP des rapports d'incidents importants liés à la cybersécurité qui font ou pourraient faire intervenir des renseignements personnels. Grâce à cette obligation supplémentaire d'informer le CIPVP dans les cas appropriés, les Ontariennes et Ontariens auront davantage confiance dans le fait que le gouvernement examine et traite comme il se doit tous les aspects des incidents de cybersécurité, y compris ceux qui touchent leur vie privée et qui, autrement, pourraient ne pas être signalés. En outre, cela permettrait au CIPVP d'avoir une vue d'ensemble des tendances possibles et de mettre à profit son expertise en cas de cyberincidents concernant les renseignements personnels des Ontariennes et des Ontariens.

L'annexe 2 du projet de loi 194 modifierait la LAIPVP en obligeant les institutions du secteur public provincial à informer le CIPVP des atteintes à la vie privée qui posent un risque réel de préjudice grave (y compris celles qui découlent d'incidents liés à la cybersécurité). Les fournisseurs de services sont déjà tenus d'aviser le CIPVP en cas d'atteinte à la vie privée en vertu du paragraphe 308 (3) de la *Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille* (LSEJF). Cependant, de nombreuses autres entités du secteur public visées par l'annexe 1, y compris tous les conseils scolaires et toutes les institutions assujetties à la LAIMPVP, ne sont pas tenues de le faire, et elles ne le seraient pas non plus après l'entrée en vigueur du projet de loi 194. Pour combler cette lacune, nous recommandons que le ministre soit tenu de signaler au CIPVP les incidents importants liés à la cybersécurité qui font ou pourraient faire intervenir des renseignements personnels.

Recommandation 8 : Amender l'annexe 1 pour enjoindre au ministre de fournir au CIPVP des copies des rapports qu'il reçoit d'institutions du secteur public en cas d'incident important lié à la cybersécurité qui fait ou pourrait faire intervenir des renseignements personnels.

[X] Le ministre fournit au commissaire à l'information et à la protection de la vie privée des copies des rapports qu'il reçoit de la part d'entités du secteur public en vertu de l'alinéa 2 (1) c), y compris des rapports élaborés par des tiers à la demande de ces entités, en ce qui concerne des incidents importants liés à la cybersécurité qui font ou pourraient faire intervenir des renseignements personnels.

Le ministère devrait préparer un rapport annuel sur ses obligations relatives aux cyberactivités

L'annexe 1 prévoit que le ministre exerce d'importantes fonctions de réglementation en ce qui concerne les cyberactivités. Les Ontariennes et Ontariens sont particulièrement intéressés et préoccupés par ces activités à risque, car elles peuvent avoir des répercussions importantes sur leur vie. Pour qu'ils aient confiance dans la manière dont sont régies ces activités, ils doivent recevoir des renseignements pertinents sur l'efficacité du régime réglementaire et sur la manière dont il est mis en œuvre.

En conséquence, nous recommandons que l'annexe 1 soit amendée pour enjoindre au ministre de préparer un rapport annuel concernant les rapports sur les cyberincidents reçus de la part des entités du secteur public au cours d'une année donnée. Ce rapport devrait renseigner la

législature et le public sur la manière dont le ministre s'acquitte de ses responsabilités, sur les tendances générales qui se dégagent au fil du temps et sur l'efficacité globale du régime de réglementation. Par exemple, le rapport annuel du ministre pourrait mentionner le nombre de rapports de cyberincidents reçus, les types de cyberincidents signalés, le nombre de rapports faisant intervenir des renseignements personnels qui ont été communiqués au Commissaire à l'information et à la protection de la vie privée, l'état général et l'issue de ces incidents, ainsi que toute tendance significative observée d'une année sur l'autre. D'autres éléments de ce rapport pourraient être décrits dans les règlements pour faire en sorte que des renseignements suffisants soient communiqués au public sans pour autant remettre en cause l'intégrité des enquêtes en cours sur la cybersécurité ou les mesures correctives prises pour renforcer la cybersécurité des systèmes des entités du secteur public.

Recommandation 9 : Amender l'annexe 1 afin d'enjoindre au ministre de produire un rapport annuel sur le nombre, les types et l'issue générale des cyberincidents signalés et sur les tendances qui se dégagent, et contenant d'autres renseignements pouvant être prescrits par règlement.

C. Recommandations portant sur la partie de l'annexe 1 qui concerne l'IA

Les technologies de l'IA promettent d'améliorer considérablement la vie des Ontariennes et des Ontariens. L'utilisation de l'IA dans le secteur public peut accélérer la prestation des services gouvernementaux, améliorer le processus décisionnel du gouvernement, renforcer l'engagement du public et contribuer à résoudre des problèmes sociaux complexes.

Les systèmes d'IA ne sont toutefois pas infaillibles, même s'ils sont très prometteurs. La mise en place de systèmes d'IA nécessite souvent de grandes quantités de renseignements personnels qui peuvent être très délicats et être partagés de manière inappropriée avec d'autres personnes[8]. Ils donnent parfois des résultats inexacts pour des raisons qu'il est presque impossible d'expliquer et de justifier[9]. Les décisions automatisées fondées sur des renseignements ou des déductions issus de systèmes d'IA peuvent avoir des répercussions importantes sur la vie des gens[10]. Ces systèmes peuvent perpétuer la discrimination et les préjugés dont font l'objet des groupes historiquement marginalisés[11].

---

[8] Federal Trade Commission (2021). *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*. Disponible à : https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

[9] Conor Dougherty (2015). « Google Photos Mistakenly Labels Black People 'Gorillas' », *The New York Times.* Disponible à : https://archive.nytimes.com/bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/.

[10] Frances Mao (2023). « Robodebt: Illegal Australian welfare hunt drove people to despair », *BBC News*. Disponible à : https://www.bbc.com/news/world-australia-66130105. Anna Holligan (2021). « Dutch Rutte government resigns over child welfare fraud scandal », *BBC News*. Disponible à : https://www.bbc.com/news/world-europe-55674146. Jeffrey Dastin (2018). « Amazon scraps secret AI recruiting tool that showed bias against women », *Reuters*. Disponible à : https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/.

[11] Ziad Obermeyer et coll. (2019). « Dissecting racial bias in an algorithm used to manage the health of populations », *Science*. Disponible à : https://www.science.org/doi/10.1126/science.aax2342. Mary Fetzer

Conscients des avantages et des risques des systèmes d'IA, le CIPVP et la Commission ontarienne des droits de la personne ont appelé le gouvernement de l'Ontario à poser des balises solides pour assurer l'utilisation responsable des systèmes d'IA. Or, dans son libellé actuel, l'annexe 1 ne comporte aucune des balises recommandées dans notre déclaration commune de mai 2023[12]. En prévoyant que les obligations des entités du secteur public seront définies ultérieurement par règlement, le gouvernement a adopté une approche semblable à celle que le gouvernement fédéral avait d'abord privilégiée dans sa *Loi sur l'intelligence artificielle et les données*, qui avait fait l'objet de vives critiques. En définitive, le gouvernement fédéral a changé sa démarche de réglementation des technologies de l'IA. Le gouvernement de l'Ontario serait bien avisé de faire de même.

Des principes fondamentaux et des balises concernant l'IA devraient être codifiés dans la loi

Les dispositions de l'annexe 1 relatives à l'IA visent à réglementer une technologie très dynamique qui est encore naissante et en pleine évolution, de sorte que le gouvernement a choisi d'établir par règlement une grande partie de ses règles de fond. Cette démarche est compréhensible dans un contexte en mutation rapide, mais il reste essentiel d'établir une approche fondée sur des principes qui s'aligne sur les normes et les valeurs de la société. Cela confère une certaine souplesse pour adapter les règles à l'évolution de la conjoncture, tout en veillant à ce que ces règles restent encadrées par des balises prévues expressément dans la loi afin de protéger les droits fondamentaux des Ontariennes et des Ontariens.

Le CIPVP recommande vivement que le projet de loi soit amendé afin d'inclure un libellé qui définit expressément les paramètres de base dans le cadre desquels seront pris les règlements éventuels. Si l'on codifie des principes normatifs rigoureux dans la loi elle-même, il sera possible de garantir au public qu'une approche solide, transparente et fondée sur des principes permettra d'exploiter les avantages potentiels de ces technologies puissantes tout en protégeant les particuliers et les groupes contre d'éventuels préjudices. Il existe dans le monde un ensemble croissant de lois, de politiques et de principes qui orientent la réglementation des systèmes d'IA (p. ex., les principes d'IA de l'OCDE[13], la résolution A/78 des Nations Unies sur l'éthique de l'IA[14], les principes directeurs internationaux du processus d'Hiroshima du G7 pour les organisations qui développent des systèmes d'IA avancés[15], les Lignes directrices en

---

(2023). « Trained AI models exhibit learned disability bias, IST researchers say », *PennState*. Disponible à : https://www.psu.edu/news/information-sciences-and-technology/story/trained-ai-models-exhibit-learned-disability-bias-ist/. Trishan Panch et coll. (2019). « Artificial intelligence and algorithmic bias: implications for health systems », *Journal of Global Health*. Disponible à : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6875681/.

[12] CIPVP et CODP (2023). *Déclaration commune du Commissaire à l'information et à la protection de la vie privée de l'Ontario et de la Commission ontarienne des droits de la personne sur l'utilisation des technologies de l'intelligence artificielle*. Disponible à : https://www.ipc.on.ca/fr/centre-des-medias/communiques/declaration-commune-du-commissaire-linformation-et-la-protection-de-la-vie-privee-de-lontario-et-de

[13] OCDE (2024). *OECD AI Principles*. Disponible à : https://oecd.ai/en/ai-principles.

[14] Nations Unies (2021). *Intelligence artificielle : 193 pays adoptent le premier accord sur l'éthique de l'IA*. Disponible à : https://news.un.org/fr/story/2021/11/1109412.

[15] G7 (2023). *Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System*. Disponible à : https://www.mofa.go.jp/files/100573471.pdf.

matière d'éthique pour une IA digne de confiance de l'Union européenne[16] citées dans la *Législation sur l'intelligence artificielle* de l'Union européenne[17], les Principes directeurs du Canada pour l'utilisation de l'IA au gouvernement[18] alignés sur l'approche commune des Nations numériques à l'égard de l'IA[19] et les mesures de protection du Colorado en lien avec l'intelligence artificielle[20]). Le gouvernement de l'Ontario a proposé son propre ensemble de principes sur l'utilisation éthique des systèmes d'IA[21].

Ainsi, il se dégage clairement dans le monde des principes universels que l'Ontario pourrait et devrait intégrer dans sa loi sur l'IA. Ces principes se reflètent dans la déclaration commune de mai 2023 du CIPVP et de la CDPO[22] et sont décrits plus loin. Pour adopter une approche qui s'harmonise avec le consensus international qui se dessine, le gouvernement devrait amender l'annexe 1 afin d'inclure des principes de haut niveau et des règles fondamentales semblables que les entités du secteur public devront suivre lorsqu'elles élaborent ou déploient des systèmes d'IA qui auront une incidence sur la population ontarienne. En souscrivant fermement à ces principes, l'Ontario se positionnerait comme un chef de file crédible et influent, désireux de devenir un centre mondial de développement et d'utilisation responsable de l'IA.

À la base, les entités du secteur public qui élaborent ou déploient des systèmes d'IA doivent s'assurer que ces systèmes présentent les caractéristiques suivantes :

- ***Validité et fiabilité* :** Avant d'être adoptées par les entités du secteur public, les technologies de l'IA devraient répondre à des normes indépendantes de validité et de fiabilité, dont les modalités pourraient être établies par règlement. Les technologies testées devraient fonctionner comme prévu dans les environnements dans lesquels elles seront utilisées. Toutes les autres obligations légales devraient être fondées sur ces tests, effectués avant le déploiement ou l'utilisation d'une technologie de l'IA et régulièrement par la suite.

- ***Sécurité* :** Les systèmes d'IA devraient être configurés pour être favorables à la vie humaine, à la santé physique et mentale, à la sécurité économique et à l'environnement.

---

[16] Commission européenne (2019). *Lignes directrices en matière d'éthique pour une IA digne de confiance*. Disponible à : https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60427.
[17] Parlement européen (2024). *Législation sur l'intelligence artificielle*. Disponible à : https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_FR.pdf.
[18] Gouvernement du Canada (2023). *Principes directeurs pour l'utilisation de l'IA au gouvernement*. Disponible à : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/principes.html.
[19] Les Nations numériques forment un forum collaboratif constitué de pays chefs de file du numérique : le Canada, le Danemark, l'Estonie, Israël, le Mexique, la Nouvelle-Zélande, le Portugal, la République de Corée, le Royaume-Uni et l'Uruguay. Précisions à : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/nations-numeriques.html.
[20] Colorado General Assembly (2024). *Consumer Protections for Artificial Intelligence*. Disponible à : https://leg.colorado.gov/bills/sb24-205.
[21] Gouvernement de l'Ontario (2023). *Principes bêta pour une utilisation éthique de l'intelligence artificielle*. Disponible à : https://www.ontario.ca/fr/page/principes-beta-pour-une-utilisation-ethique-de-lintelligence-artificielle.
[22] CIPVP et CODP (2023). *Déclaration commune du Commissaire à l'information et à la protection de la vie privée de l'Ontario et de la Commission ontarienne des droits de la personne sur l'utilisation des technologies de l'intelligence artificielle*. Disponible à : https://www.ipc.on.ca/fr/centre-des-medias/communiques/declaration-commune-du-commissaire-linformation-et-la-protection-de-la-vie-privee-de-lontario-et-de.

Ils devraient être surveillés et évalués tout au long de leur durée de vie afin de s'assurer qu'ils demeurent favorables à ces objectifs et qu'ils peuvent résister à des événements inattendus ou à des manœuvres délibérées qui les amèneraient à se comporter de manière préjudiciable, non souhaitée ni prévue par les créateurs, les opérateurs ou les utilisateurs de ces systèmes d'IA.

- ***Protection de la vie privée*** **:** Les technologies d'IA devraient être élaborées ou adoptées selon une approche fondée sur la protection intégrée de la vie privée, qui prévoit et atténue les risques pour la vie privée des particuliers et des groupes. Cela signifie notamment que la collecte, le traitement, la conservation et l'utilisation de données personnelles en lien avec les systèmes d'IA, y compris les données d'entraînement, doivent être clairement autorisés par la loi. Les systèmes doivent comporter des mesures visant à garantir l'exactitude des résultats de l'IA et à protéger toutes les déductions sur les personnes qui découlent de ces résultats comme s'il s'agissait de renseignements personnels. Les systèmes d'IA doivent également être conçus pour protéger les renseignements personnels contre les accès non autorisés ou les menaces liées à la cybersécurité. Les particuliers devraient être informés de l'utilisation prévue de la technologie de l'IA aux fins du traitement de leurs renseignements personnels et, le cas échéant, avoir la possibilité de refuser une décision automatisée pour privilégier un décideur humain.

- ***Transparence*** **:** Les entités du secteur public devraient adopter des politiques et des pratiques qui rendent visible, intelligible et compréhensible le fonctionnement des technologies de l'IA. Dans ce but, ces entités devraient conserver suffisamment de renseignements techniques sur les technologies de l'IA qu'elles utilisent afin de pouvoir rendre compte de la manière dont les décisions sont prises. Les particuliers devraient être informés des décisions qui ont été prises à leur sujet à l'aide de l'IA. Ils devraient également être informés lorsqu'ils interagissent avec une technologie de l'IA et lorsque les renseignements qui leur sont présentés ont été générés par des systèmes d'IA. Le degré de transparence des entités du secteur public peut varier selon qu'il s'adresse au public, aux particuliers ou aux groupes directement concernés par les systèmes d'IA, ou aux organismes de réglementation chargés de les superviser.

- ***Reddition de comptes*** **:** Les entités du secteur public doivent mettre en place une structure de gouvernance solide pour l'élaboration, le déploiement, l'utilisation, la réaffectation ou la mise hors service des systèmes d'IA, prévoyant des rôles et des responsabilités clairement définis. Elles devraient être tenues de procéder à des évaluations de l'incidence algorithmique, y compris des évaluations de l'impact sur la vie privée, afin de cerner les risques liés aux algorithmes et les moyens de les atténuer. Elles devraient préciser et documenter leurs choix en matière de conception et d'application de leurs systèmes d'IA, ainsi que les décisions prises à l'égard de groupes ou de particuliers à l'aide des résultats de l'IA. Les particuliers doivent être en mesure de contester l'exactitude des décisions prises à leur sujet et d'obtenir réparation lorsqu'ils estiment qu'elles ont eu une incidence négative sur eux. Les entités du secteur public devraient être soumises à l'examen d'un organisme de surveillance indépendant habilité à faire respecter ces principes et à exiger que ces entités prennent des mesures correctives, le cas échéant.

- ***Affirmation des droits de la personne :*** Les technologies de l'IA doivent être conçues pour être justes et équitables. Elles doivent respecter et affirmer les droits individuels et

collectifs. Elles doivent également être conçues de manière à lutter contre les discriminations et les préjugés historiques et à y remédier, afin que les particuliers et les communautés concernés par les systèmes d'IA ne fassent pas l'objet d'une discrimination permanente fondée sur l'application égale de la logique d'une technologie de l'IA donnée ou de ses extrants.

Recommandation 10 : Renforcer l'annexe 1 en codifiant des principes clairs qui serviront de balises encadrant l'utilisation responsable des systèmes d'IA par les entités du secteur public. La codification de ces balises, en plus de la disposition d'objet proposée dans la recommandation 1, fournirait les garanties nécessaires pour gagner et conserver la confiance des Ontariennes et des Ontariens dans l'utilisation des systèmes d'IA. Des précisions pourraient être apportées par le biais de règlements ou de normes techniques, ce qui permettrait d'adopter une approche réglementaire plus souple et plus évolutive.

Une approche réglementaire fondée sur le risque devrait être adoptée

Plusieurs régimes de réglementation de l'IA qui voient le jour dans le monde suivent une approche fondée sur le risque, selon laquelle les règles et les obligations imposées aux organisations qui élaborent ou déploient des systèmes d'IA sont plus ou moins exigeantes, selon le niveau de risque ou les préjudices possibles pour les particuliers et les groupes. Par exemple, la *Législation sur l'intelligence artificielle* de l'Union européenne[23], les mesures de protection du Colorado en lien avec l'intelligence artificielle[24], le cadre de gestion des risques de l'IA du National Institute of Standards and Technology (NIST)[25] et la *Loi sur l'intelligence artificielle et les données* (LIAD) du Canada[26] contenue dans le projet de loi C-27 imposent des exigences plus strictes et des mesures de surveillance et d'application plus rigoureuses à mesure que le degré de risque ou de préjudice éventuel augmente.

L'annexe 1 du projet de loi 194, dans la mesure où elle vise à réglementer les systèmes d'IA élaborés ou adoptés par des entités du secteur public, devrait être fondée sur une approche semblable axée sur le risque. Une telle approche apporterait la souplesse nécessaire à l'adoption et au déploiement de systèmes d'IA, tout en assurant aux particuliers et aux groupes un niveau de protection proportionnel de leur sécurité et de leurs droits.

Recommandation 11 : Modifier l'annexe 1 pour adopter explicitement un cadre fondé sur le risque. Ce cadre devrait évaluer l'incidence éventuelle et la probabilité des préjudices associés aux différents systèmes d'IA, en veillant à ce que les systèmes qui présentent un risque plus élevé de préjudice involontaire fassent l'objet d'une surveillance plus stricte que ceux qui sont classés comme présentant un risque moins élevé.

---

[23] Parlement européen (2024). *Législation sur l'intelligence artificielle*. Disponible à : https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_FR.pdf.
[24] Colorado General Assembly (2024). *Consumer Protections for Artificial Intelligence*. Disponible à : https://leg.colorado.gov/bills/sb24-205.
[25] National Institute of Standards and Technology (2023). *AI Risk Management Framework*. Disponible à : https://www.nist.gov/itl/ai-risk-management-framework.
[26] Gouvernement du Canada (2023). *Loi sur l'intelligence artificielle et les données (LIAD)*. Disponible à : https://www.parl.ca/legisinfo/fr/projet-de-loi/44-1/c-27.

Certaines utilisations de l'IA devraient être interdites dans la loi

Malgré la recommandation 11, nous pensons qu'il existe un seuil de risque clair, ou certains préjudices, au-delà desquels nous ne devrions pas nous aventurer en tant que société. Tout comme il est important de prescrire les fins auxquelles les entités du secteur public peuvent utiliser des systèmes d'IA en respectant certaines balises, il faut également prescrire les fins auxquelles elles ne peuvent pas utiliser de tels systèmes. Le paragraphe 5 (6) de l'annexe 1 prévoit que le gouvernement peut interdire par règlement certaines utilisations des technologies de l'IA. Le CIPVP est favorable à la définition de situations où il serait interdit pour les entités du secteur public d'utiliser ces technologies d'une façon qui serait inacceptable ou trop dangereuse pour la société. Nous croyons que certaines utilisations sont à ce point rejetées par la population ontarienne qu'elles devraient être interdites d'ores et déjà par la loi; d'autres pourront être proscrites plus tard par règlement.

L'annexe 1 du projet de loi 194 devrait établir clairement et explicitement les fins auxquelles il serait interdit aux entités du secteur public d'utiliser des systèmes d'IA. L'article 5 de la *Législation sur l'intelligence artificielle* de l'Union européenne codifie une liste de pratiques d'IA interdites[27]. Nous recommandons à l'Ontario d'envisager d'interdire une liste semblable d'utilisations que les Ontariennes et Ontariens jugeraient tout à fait inacceptables, et qui seraient très peu susceptibles de changer avec le temps étant donné notre engagement inébranlable à l'égard des droits de la personne et des principes fondamentaux d'une société libre et démocratique.

Recommandation 12 : Amender l'annexe 1 du projet de loi 194 afin d'y inclure une liste d'utilisations interdites des systèmes d'IA, qui pourrait être étoffée par règlement. Les utilisations interdites des technologies devraient être évaluées en fonction des principes fondamentaux de l'IA que le CIPVP propose dans la recommandation 10.

Recommandations sur les technologies numériques touchant les particuliers âgés de moins de 18 ans

La troisième partie de l'annexe 1, qui s'appelle *Technologie numérique touchant les particuliers âgés de moins de 18 ans*, établirait un régime de réglementation de l'information numérique concernant des particuliers de moins de 18 ans que les conseils scolaires et les sociétés d'aide

[27] Voici des exemples d'utilisations expressément interdites des technologies de l'IA en vertu de la *Législation sur l'intelligence artificielle* de l'UE : 1) un système d'IA qui a recours à des techniques subliminales, au-dessous du seuil de conscience d'une personne, avec pour objectif ou effet d'altérer substantiellement le comportement d'une personne, d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique important à cette personne ou à une autre personne; 2) un système d'IA qui classifie des personnes pour produire une note sociale en fonction de leur comportement social de caractéristiques personnelles ou de personnalité connues, déduites ou prédites, conduisant à un traitement préjudiciable ou défavorable; 3) l'utilisation d'un système d'IA qui crée ou développe des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant d'Internet ou de la vidéosurveillance; 4) un système d'IA utilisé pour évaluer la probabilité qu'une personne commette une infraction pénale, uniquement sur la base du profilage de cette personne ou de l'évaluation de ses traits de personnalité ou caractéristiques.
Pour en savoir davantage, voir : EU Artificial Intelligence Act. (2024). *Article 5 : Pratiques interdites en matière d'intelligence artificielle*. Disponible à : https://artificialintelligenceact.eu/fr/article/5/.

à l'enfance, peuvent recueillir, utiliser, conserver ou divulguer, et des types de technologies numériques qu'ils peuvent mettre à la disposition des enfants et des jeunes.

Comme *Les enfants et les jeunes dans un monde numérique* compte parmi les priorités stratégiques de mon bureau, je félicite le gouvernement de vouloir renforcer les protections conférées aux enfants et aux jeunes. Cependant, le modèle proposé à l'annexe 1 présente plusieurs failles.

Les mesures de protection de la vie privée des enfants prévues dans les lois ontariennes actuelles sur la protection de la vie privée devraient être renforcées

Surtout, nous sommes très préoccupés par le chevauchement entre le régime réglementaire proposé, qui relèverait du ministre, et mon mandat actuel sur *la même activité réglementée* en vertu des lois ontariennes sur l'accès à l'information et la protection de la vie privée. Ce chevauchement pourrait donner lieu à l'adoption de normes redondantes ou divergentes par le ministre d'une part et mon bureau d'autre part, ce qui susciterait de la confusion, de l'incohérence et de l'incertitude au sein des entités réglementées[28]. Par exemple, des règlements pris en application de l'article 9 et de l'alinéa 10 a) de l'annexe 1 prescrivant comment les conseils scolaires et les sociétés d'aide à l'enfance peuvent ou ne peuvent pas recueillir, utiliser, conserver ou divulguer de l'information numérique concernant les enfants et les jeunes de moins de 18 ans pourraient aller à l'encontre des décisions rendues et des orientations adoptées par mon bureau aux termes de la LAIMPVP et de la partie X de la LSEJF en ce qui concerne les mêmes activités.

C'est pourquoi nous recommandons vivement que l'article 9 et l'alinéa 10 a) soient supprimés de l'annexe 1 et que les mesures supplémentaires de protection de la vie privée que ces dispositions visent à introduire soient étudiées plus en profondeur et intégrées plutôt dans la LAIPVP, la LAIMPVP et la partie X de la LSEJF. Il serait possible ainsi de renforcer les mesures de protection et les obligations qui existent déjà quant à la collecte, à l'utilisation, à la conservation et à la divulgation de renseignements personnels, y compris ceux qui concernent des enfants et des jeunes, et de créer un régime plus cohérent et uniforme au lieu d'instaurer des règles éventuellement contradictoires. Mon bureau est disposé à fournir des conseils sur le meilleur moyen d'y parvenir.

Recommandation 13 : Supprimer l'article 9 et l'alinéa 10 a) de l'annexe 1 et renforcer plutôt les dispositions relatives à la protection de la vie privée figurant dans la LAIPVP, la LAIMPVP et la partie X de la LSEJF afin de protéger les enfants et les jeunes dans le cadre d'un régime réglementaire de protection de la vie privée plus cohérent et homogène.

[28] La professeure Teresa Scassa, dans ses observations sur le projet de loi 194, souligne également que la loi pourrait donner lieu à une situation où [traduction] « les règlements pourraient établir des exigences ou des normes moins strictes que celles que prévoient la LAIPVP ou la LAIMPVP, créant ainsi un régime inutilement confus et déroutant ». Elle recommande de reporter dans un autre texte de loi les articles 9 (règlements pris par le lieutenant-gouverneur en conseil) et 10 (règlements du ministre : normes techniques) pour éviter de compliquer le régime de réglementation actuel.

L'application des directives et règlements ministériels sur les technologies numériques mises à la disposition des particuliers âgés de moins de 18 ans devrait être élargie

Par ailleurs, nous sommes favorables aux autres dispositions de l'annexe 1, à savoir l'alinéa 10 b) et l'article 11, qui prévoient que le ministre peut prendre des règlements prescrivant des normes techniques et des directives concernant les technologies numériques mises à la disposition des particuliers âgés de moins de 18 ans. Le CIPVP reconnaît que des normes techniques pourraient rehausser les protections conférées aux enfants et aux jeunes de la province si elles étaient mises en œuvre de manière à protéger la vie privée et à respecter les valeurs que sont l'autonomie personnelle, la dignité et l'autodétermination, conformément à la disposition d'objet que nous proposons dans la recommandation 1.

En outre, l'adoption systématique de normes techniques a pour avantage supplémentaire de renforcer le pouvoir de négociation des conseils scolaires et des sociétés d'aide à l'enfance à l'égard des fournisseurs externes de plateformes numériques. Les conseils et sociétés pourraient se référer à ces normes techniques lorsqu'ils négocient avec ces fournisseurs l'ajout de certaines mesures de protection ou la suppression de certaines fonctionnalités de leurs logiciels afin de se conformer aux lois ontariennes.

Cependant, dans son libellé actuel, la partie *Technologie numérique touchant les particuliers âgés de moins de 18 ans* de l'annexe 1 ne s'applique qu'aux conseils scolaires et aux sociétés d'aide à l'enfance, et non à d'autres fournisseurs de services à l'enfance et à la famille et entités du secteur public dont on pourrait raisonnablement s'attendre à ce qu'elles mettent des technologies à la disposition d'enfants de moins de 18 ans. Ainsi, le projet de loi sous sa forme actuelle exclut les bibliothèques publiques, les garderies et camps de jour municipaux ainsi que les foyers de groupe. Cette exclusion ajoute à l'incohérence et à l'incertitude de la réglementation, car certaines organisations seraient réglementées et d'autres pas. De plus, elle donnerait lieu à des injustices et à des inégalités, en procurant une protection variable aux enfants et aux jeunes selon l'entité du secteur public avec qui ils interagissent.

C'est pourquoi nous recommandons que les entités du secteur public visées par les directives et règlements du ministre sur les normes techniques concernant les technologies numériques mises à la disposition des particuliers âgés de moins de 18 ans comprennent également tous les fournisseurs de services au sens de la LSEJF, ainsi que toutes les autres institutions municipales et provinciales du secteur public dont on pourrait raisonnablement s'attendre à ce qu'elles mettent de pareilles technologies à la disposition des enfants et des jeunes.

Recommandation 14 : Amender l'annexe 1 du projet de loi 194 afin que les directives et règlements du ministre sur les normes techniques concernant les technologies numériques mises à la disposition des particuliers âgés de moins de 18 ans s'appliquent à tous les fournisseurs de services au sens de la LSEJF ainsi qu'à toutes les autres institutions du secteur public dont on pourrait raisonnablement s'attendre à ce qu'elles mettent de pareilles technologies à la disposition des enfants et des jeunes.

L'ANNEXE 2 DU PROJET DE LOI 194 : MODIFICATIONS À LA *LOI SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DE LA VIE PRIVÉE*

Le CIPVP est ravi de constater que des modifications tant attendues à la LAIPVP pourraient enfin l'aligner sur la plupart des autres lois modernes sur la protection de la vie privée et renforcer les protections dont les Ontariennes et les Ontariens ont besoin et qu'ils méritent à l'ère numérique. Ces modifications comprennent des évaluations de l'impact sur la vie privée, l'obligation de signaler les atteintes à la vie privée et une application plus stricte de la loi. Cependant, il reste d'autres lacunes importantes à combler. Avant que ne soit arrêté le libellé définitif de l'annexe 2 du projet de loi 194, nous recommandons vivement certains amendements afin de ne pas manquer cette occasion de bien faire les choses.

Des principes de minimisation des données devraient être instaurés

La minimisation des données est un principe fondamental de protection de la vie privée qui se retrouve dans la plupart des lois modernes sur la protection de la vie privée et qui permet de se prémunir contre la collecte, l'utilisation et la divulgation excessives de renseignements personnels. La LPRPS et la partie X de la LSEJF contiennent toutes deux une disposition relative à la minimisation des données, de même que la LAIPVP, bien qu'uniquement en ce qui concerne la partie III.1[29]. Nous ajoutons également un principe de minimisation des données à la partie III de la LAIPVP.

La minimisation des données est une approche rigoureuse selon laquelle le gouvernement doit recueillir, utiliser et divulguer à des fins légitimes le moins de renseignements personnels possible. Elle consiste généralement en l'exigence générale pour les organisations de ne pas recueillir, utiliser ou divulguer plus de renseignements personnels qu'il n'est raisonnablement nécessaire pour réaliser la fin visée. Elle n'empêche pas ces organisations de remplir leurs fonctions légitimes; elle vise seulement à limiter la quantité de renseignements personnels qui interviennent dans le cadre de ces fonctions.

Recueillir, utiliser ou divulguer uniquement les renseignements personnels qui sont nécessaires est un moyen fondamental de respecter la vie privée des particuliers. Ainsi, l'institution doit tenir compte des fins visées et préciser à quoi les renseignements personnels pourraient servir ou non. Il est possible ainsi d'éviter, par exemple, la collecte d'une quantité exagérée de renseignements personnels et de multiplier les fins auxquels ils servent. La minimisation des données représente aussi un moyen efficace de protéger les institutions contre les effets dévastateurs des atteintes à la vie privée. En effet, quand on recueille moins de renseignements personnels, on en risque la perte ou la divulgation d'une quantité moindre en cas d'atteinte à la vie privée. Le fait d'avoir moins de données à conserver et à gérer de façon sécurisée rapporte aussi d'autres avantages, car les ressources requises sont moindres, de même que les coûts techniques connexes.

La minimisation des données est une norme universelle et moderne de protection des données, et nous recommandons vivement d'ajouter une disposition à cet effet à la partie III de la LAIPVP par l'entremise de l'annexe 2 proposée.

---

[29] À l'heure actuelle, la minimisation des données aux termes de la partie III.1 de la LAIPVP s'applique uniquement aux activités d'un petit nombre de services désignés d'intégration des données, alors qu'aux termes de l'article 30 de la LPRPS et des articles 283 et 287 de la LSEJF, elle fait l'objet d'une application plus générale.

Recommandation 15 : Amender l'annexe 2 en incluant dans la partie III de la LAIPVP un principe de minimisation des données semblable à celui qui existe déjà dans la LPRPS, la partie X de la LSEJF et la partie III.1 de la LAIPVP.

> ***XXX (1) Une institution ne doit pas recueillir, utiliser ou divulguer de renseignements personnels à une fin que d'autres renseignements permettent de réaliser.***
>
> ***(2) Une institution ne doit pas recueillir, utiliser ou divulguer plus de renseignements personnels qu'il n'est raisonnablement nécessaire pour réaliser la fin visée.***
>
> ***(3) Le présent article ne s'applique pas aux renseignements personnels que la loi oblige une institution à recueillir, à utiliser ou à divulguer.***

Les exigences relatives aux évaluations de l'impact sur la vie privée pourraient être renforcées

Si elle était adoptée, l'annexe 2 modifierait la LAIPVP afin d'obliger les institutions provinciales à effectuer une évaluation de l'impact sur la vie privée (EIVP) avant de recueillir des renseignements personnels, et à fournir au CIPVP une copie de cette EIVP sur demande. Il s'agit là d'un changement très positif. Les EIVP sont essentielles à la *protection intégrée de la vie privée*. Elles révèlent des risques possibles pour la vie privée, et elles permettent aux décideurs d'évaluer et d'anticiper les risques graves dès le départ, afin de les résoudre ou de les atténuer de manière proactive avant de déployer une initiative ou un programme nouveau ou modifié, évitant ainsi des atteintes coûteuses à la vie privée et une perte de confiance du public.

Cependant, aux termes de la modification proposée, les institutions pourraient commencer à recueillir des renseignements personnels « s'il est impossible de mettre en œuvre les mesures avant de les recueillir ». Dans un tel cas, ces mesures peuvent être prises « dans un délai raisonnable ». En vertu de cette disposition proposée, les renseignements personnels délicats des Ontariennes et des Ontariens pourraient être recueillis et exposés à un risque important pendant une période indéterminée avant que ce risque ne soit atténué. Nous sommes conscients du fait que dans certaines situations, des exceptions pourraient être justifiées, mais la disposition proposée est trop permissive sous sa forme actuelle. Nous recommandons que la possibilité de recueillir des données personnelles avant la mise en place de mesures d'atténuation soit limitée aux situations où le risque pour la vie privée est faible.

Recommandation 16 : Amender le paragraphe 4 (2) de l'annexe 2 (proposant d'ajouter de nouvelles dispositions à l'article 38 de la LAIPVP) pour circonscrire les situations où une institution peut recueillir des renseignements personnels concernant des Ontariennes ou des Ontariens avant d'avoir franchi les étapes requises pour minimiser les risques pour la vie privée qui ont été relevées dans une EIVP.

> *38 (4) La personne responsable d'une institution veille à ce que les mesures visées à la disposition 9 du paragraphe (3) soient mise* [sic] *en œuvre :*

a) avant de recueillir les renseignements personnels visés à ce paragraphe,
b) dans un délai raisonnable après avoir recueilli les renseignements personnels, s'il est impossible de mettre en œuvre les mesures avant de les recueillir ***et si les risques pour la vie privée des particuliers sont faibles.***

L'annexe 2 du projet de loi 194 obligerait également les institutions à modifier une EIVP en cas de modification importante des fins auxquelles les renseignements personnels sont utilisés ou divulgués. Cette exigence est effectivement essentielle pour assurer la tenue à jour des EIVP en cas de changement important apporté à un programme, à une initiative ou à une activité, pour que les institutions aient une idée précise des risques en cause.

Toutefois, les EIVP devraient être mises à jour chaque fois qu'un changement important intervient dans l'un des facteurs initialement pris en compte dans le cadre de l'EIVP, et non seulement en cas de modification des fins auxquelles les renseignements personnels sont utilisés ou divulgués. Il pourrait s'agir de tout changement important concernant l'autorité légale de l'institution, les types ou sources de renseignements personnels à recueillir, les fonctions des personnes qui auront accès à l'information, l'une ou l'autre des limites ou restrictions prévues, la période de conservation des renseignements personnels ou les mesures de précaution ou pratiques suivies pour protéger les renseignements personnels. Si on oblige la mise à jour des EIVP uniquement lorsqu'on modifie les fins auxquelles les renseignements personnels sont utilisés ou divulgués, de nouveaux risques pour la vie privée découlant de ces changements importants pourraient passer inaperçus et ne pas être atténués.

Recommandation 17 : Amender le paragraphe 4 (2) de l'annexe 2 pour accroître le nombre de situations dans lesquelles les EIVP doivent être mis à jour en vertu du paragraphe 38 (5) proposé de la LAIPVP.

38 (5) Sauf disposition contraire des règlements, avant d'apporter toute modification importante aux ~~fins auxquelles les renseignements personnels visés~~ ***renseignements énumérés*** *au paragraphe (3) ~~sont utilisés ou divulgués~~, la personne responsable d'une institution fait ce qui suit :*

a) elle met à jour l'évaluation préparée en application du paragraphe (3) pour tenir compte de la modification proposée ~~et énoncer l'utilisation ou la divulgation prévue proposée~~;
b) elle met en œuvre les mesures supplémentaires déterminées en application de la disposition 9 du paragraphe (3).

Les motifs des plaintes de particuliers devraient être élargis

L'annexe 2 du projet de loi 194 modifierait la LAIPVP pour préciser que les particuliers ont le droit de porter plainte au CIPVP en cas d'atteinte à la vie privée. Ce changement était attendu depuis longtemps et nous sommes heureux de voir que cette lacune de la loi est enfin comblée. Toutefois, telle qu'elle est actuellement proposée, l'annexe 2 semble n'accorder le droit de déposer une telle plainte qu'aux particuliers qui ont été informés d'une atteinte à la vie privée. Par exemple, si un particulier était mis au courant d'une atteinte possible à sa vie privée sans avoir reçu un avis officiel d'atteinte à la vie privée de la part de l'institution (p. ex., si un employé a consulté des renseignements sans autorisation, ou si l'institution a fait l'objet d'un autre type

d'accès non autorisé qu'elle ignorait ou dont elle n'a pas informé le particulier), il n'aurait pas le droit de porter plainte. Un particulier ayant des motifs de croire qu'une institution recueille ou conserve ses renseignements personnels abusivement ne pourrait pas porter plainte non plus.

Les motifs pour lesquels les particuliers peuvent déposer une plainte auprès du CIPVP devraient être élargis pour inclure toute situation dans laquelle un particulier a des motifs raisonnables de croire qu'une institution n'a pas respecté une obligation prévue à la partie III de la LAIPVP, qu'il ait reçu ou non un avis officiel d'atteinte à la vie privée de la part de l'institution. Cela permettrait d'aligner plus étroitement la LAIPVP sur le droit général des particuliers de porter plainte en vertu de la LPRPS et de la LSEJF et d'autres lois sur la protection de la vie privée en vigueur au Canada.

Recommandation 18 : Amender l'article 6 de l'annexe 2 afin d'élargir les motifs de plainte en matière de protection de la vie privée par adjonction du nouveau paragraphe 40.1 (4.1) à la LAIPVP et apporter un amendement corrélatif au nouveau paragraphe 40.1 (5) proposé de la LAIPVP.

> ***Plaintes en matière de protection de la vie privée***
>
> *40.1* ***(4.1) Quiconque a des motifs raisonnables de croire qu'une autre personne a contrevenu à une disposition de la présente partie ou est sur le point de le faire peut porter plainte devant le commissaire.***
>
> *Délai de dépôt des plaintes*
>
> *40.1 (5) Toute plainte visée au paragraphe (4**.1**) est faite par écrit et déposée auprès du commissaire au plus tard un an après que l'objet de la plainte a été porté pour la première fois à l'attention du plaignant ou après qu'il aurait dû raisonnablement être porté à son attention, selon le plus court de ces délais.*

La loi devrait conférer des pouvoirs d'enquête

L'annexe 2 devrait conférer certains pouvoirs d'enquête au commissaire afin de permettre à ce dernier d'examiner des plaintes ou autres affaires concernant la protection de la vie privée aux termes de la LAIPVP. Plus précisément, l'annexe 2 devrait permettre au commissaire d'exiger la production de renseignements et de documents qui se rapportent à l'objet de l'examen et dont une institution a la garde ou le contrôle, et d'imposer aux dirigeants, employés, experts-conseils et mandataires de l'institution l'obligation correspondante de coopérer à l'examen.

Cette disposition est une bonne première étape, mais elle est insuffisante pour mener une enquête efficace dans le contexte actuel, de plus en plus numérique. Les enquêtes en matière de protection de la vie privée font intervenir généralement des technologies de l'information (IT) complexes et de multiples parties qui ne sont pas nécessairement des institutions au sens de la LAIPVP. Par exemple, il pourrait être nécessaire de pénétrer dans un lieu et d'examiner sur place des systèmes de TI complexes afin de bien déterminer les vulnérabilités technologiques qui auraient pu donner lieu à une atteinte à la vie privée. De plus, il est essentiel pour le commissaire de pouvoir assigner à comparaître et interroger sous serment des personnes autres que l'institution, y compris des fournisseurs externes de traitement des données ou des personnes dont on soupçonne qu'elles auraient pu commettre des actes malveillants ayant

donné lieu à l'atteinte à la vie privée afin de déterminer la circulation des données et de mener une enquête exhaustive auprès de l'ensemble des intervenants impliqués.

Ces pouvoirs sont déjà prévus aux paragraphes 60 (1) et 59 (2) de la LPRPS, aux paragraphes 320 (1) et 319 (2) de la LSEJF et dans d'autres régimes de protection de la vie privée dans l'ensemble du pays. Ils existent également déjà en vertu du paragraphe 52 (4) de la LAIPVP dans le cadre du processus d'enquête sur les appels touchant l'accès à l'information. Bien que ces pouvoirs soient utilisés rarement, il s'agit d'outils essentiels pour accroître l'efficacité des enquêtes, surtout lorsque les parties sont récalcitrantes ou peu coopératives.

Recommandation 19 : Amender l'article 7 de l'annexe 2 en élargissant la portée des pouvoirs d'enquête dont le commissaire a besoin pour effectuer les examens des pratiques relatives aux renseignements aux termes de l'article 49.0.1 proposé de la LAIPVP.

> *Examen par le commissaire des pratiques relatives aux renseignements*
> *49.0.1 (1) Le commissaire peut ~~examiner~~**déterminer la conformité d'une personne à la présente partie** ~~les pratiques relatives aux renseignements d'une institution~~ s'il a reçu une plainte aux termes du paragraphe 40.1 (4**.1**) ou qu'il a des motifs de croire qu'il n'est pas **ou ne sera pas** satisfait aux exigences de la présente partie.*
>
> *Pouvoirs du commissaire*
> *(6) Le commissaire peut exiger la production de renseignements et de documents qui se rapportent à l'objet de l'examen ~~et qui sont sous la garde ou le contrôle d'une institution~~.*
>
> ***Interrogatoire sous serment***
> ***(6.1) Le commissaire peut assigner à comparaître et interroger sous serment la personne qui, à son avis, pourrait avoir des renseignements relatifs à l'examen mené en vertu de la présente partie. Il peut faire prêter serment à cette fin.***
>
> ***Accès***
> ***(6.2) Lorsqu'il effectue un examen en vertu de la présente partie, le commissaire peut, à toute heure raisonnable et sans mandat ni ordonnance du tribunal, pénétrer dans un lieu autre qu'un logement pour effectuer une inspection afin de déterminer si les exigences en matière de sécurité y sont respectées.***
>
> ***Preuve***
> ***(6.3) Lorsqu'il effectue un examen en vertu de la présente partie, le commissaire peut recevoir et accepter les éléments de preuve et autres renseignements qu'il estime appropriés, qu'ils soient présentés sous serment, par affidavit ou autrement et qu'ils soient ou seraient admissibles ou non devant un tribunal judiciaire.***
>
> *Ordonnances*
> *(7) ~~If, a~~**A**près avoir donné à la personne responsable de l'institution **et à toute autre personne concernée** l'occasion d'être entendue**, le commissaire peut enjoindre à toute personne de s'acquitter d'une obligation imposée par la présente partie et, s'il** établit qu'une pratique relative aux renseignements contrevient à la présente partie, il peut ordonner à la personne responsable de prendre l'une ou l'autre des mesures suivantes :*

1. Cesser la pratique relative aux renseignements.
2. Modifier la pratique relative aux renseignements, selon les indications du commissaire.
3. Retourner, transférer ou détruire les renseignements personnels recueillis ou conservés dans le cadre de la pratique relative aux renseignements.
4. Mettre en œuvre une pratique relative aux renseignements différente, selon les indications du commissaire.
5. Faire une recommandation concernant la façon dont la pratique relative aux renseignements pourrait être améliorée.

Restriction applicable à certaines ordonnances
(8) Le commissaire ne peut ordonner, en vertu du paragraphe (5), que soient prises des mesures allant au-delà de ce qui est raisonnablement nécessaire pour se conformer à la présente partie.

Procédures
(9) La Loi sur l'exercice des compétences légales ne s'applique pas à un examen prévu ~~au présent article~~ ***à la présente partie, et le commissaire peut établir les règles de procédure qu'il estime nécessaires****.*

Permettre au commissaire de divulguer des renseignements au besoin

Actuellement, la LAIPVP impose au commissaire l'une des dispositions les plus restrictives en matière de confidentialité de toutes les lois canadiennes sur la protection de la vie privée. La LAIPVP ne prévoit aucune exception à l'obligation du commissaire de ne pas divulguer les renseignements portés à sa connaissance dans l'exercice de ses attributions en vertu de cette loi ou de toute autre loi.

L'annexe 2 du projet de loi 194 changerait cette situation en permettant au commissaire de divulguer des renseignements à ses homologues fédéraux, provinciaux et territoriaux pour coordonner des activités, notamment en matière d'exécution de la loi et d'élaboration de politiques, pour faire en sorte que les renseignements personnels soient protégés de la façon la plus uniforme possible dans les différents territoires de compétence. Il s'agit d'une modification très opportune que mon bureau appuie sans réserve.

L'annexe 2 permettrait également au commissaire de divulguer des renseignements si la divulgation est permise à une fin prescrite. On ne sait pas encore quelles seront ces exceptions, ou quand elles pourraient être adoptées par voie de résolution. Le paragraphe 68 (3) de la LPRPS et le paragraphe 328 (3) de la LSEJF, par contre, comportent des dispositions plus explicites qui permettent au commissaire de divulguer des renseignements qui sont portés à sa connaissance dans l'exercice de ses fonctions, si la divulgation est exigée à cette fin.

Ainsi, des renseignements pourraient être divulgués aux parties, et parfois à des tiers, pour faire enquête ou pour établir les motifs de constatations, de recommandations et d'ordonnances. Il pourrait également être nécessaire de divulguer des renseignements à un tribunal dans le contexte d'une révision judiciaire ou d'autres instances. Le commissaire devrait être tenu de divulguer des renseignements à d'autres institutions publiques qui en ont besoin pour atténuer les conséquences d'une atteinte à la vie privée ou d'un incident majeur lié à la cybersécurité, par exemple, ou au procureur général pour qu'il puisse intenter des poursuites en cas

d'infraction à la loi. Surtout, le commissaire pourrait devoir divulguer des renseignements dans l'intérêt public à des fins d'information du public, de reddition de comptes et de transparence. Si le commissaire dispose de pouvoirs supplémentaires pour faire enquête sur les plaintes relatives à la protection de la vie privée, notamment à la suite d'atteintes à la vie privée très médiatisées qui touchent des centaines de milliers de personnes, la population ontarienne s'attendra à être informée de l'état et de l'issue des enquêtes.

Recommandation 20 : Amender l'article 9 de l'annexe 2 pour éliminer toute ambiguïté concernant le fait que le commissaire peut communiquer les renseignements nécessaires à l'exercice de ses attributions en vertu du paragraphe 55 (1) de la LAIPVP.

> *55 (1) Le commissaire ou la personne qui agit pour son compte ou sous son autorité ne peuvent divulguer les renseignements portés à leur connaissance dans l'exercice de leurs attributions en vertu de la présente loi ou de toute autre loi,* ***sauf si la divulgation est requise pour l'exercice de ces attributions ou*** *permise à une fin prescrite.*

Si le projet de loi 194 est adopté en l'état, nous demandons instamment au gouvernement d'accélérer l'élaboration du règlement relatif aux exceptions à l'obligation de confidentialité du commissaire afin qu'il entre en vigueur dès la promulgation de la loi.

Une règle concernant les destinataires devrait être incluse

Les institutions publiques confient de plus en plus certaines fonctions à des fournisseurs externes pour remplir le mandat que leur confère la loi. Ces scénarios supposent souvent le traitement de renseignements personnels par des organisations externes qui ne sont pas des institutions assujetties à la LAIPVP.

Une *règle concernant les destinataires* permettrait de faire en sorte que lorsque des institutions partagent des renseignements personnels concernant des Ontariennes et des Ontariens avec un destinataire tiers, ce dernier ne puisse pas utiliser ces renseignements à d'autres fins, par exemple, les exploiter à des fins commerciales ou pour son propre bénéfice. Une telle règle obligerait également les tiers à informer les institutions en cas d'atteinte à la vie privée. Il arrive que les institutions incluent de telles restrictions et obligations dans leurs accords contractuels avec des fournisseurs externes, mais cela ne se fait pas toujours, et ces modalités ne sont pas toujours faciles à négocier ou à faire respecter. L'imposition d'une obligation légale directe aux destinataires limitant l'utilisation qu'ils peuvent faire des renseignements personnels et les obligeant à informer l'institution en cas d'atteinte à la vie privée aiderait les institutions à renforcer leurs accords avec ces fournisseurs ou à en combler les lacunes.

Une telle *règle concernant les destinataires* dans la LAIPVP correspondrait également à une obligation semblable qui existe déjà à l'article 49 de la LPRPS. Elle préciserait que lorsqu'une institution divulgue des renseignements personnels à un destinataire (qui n'est pas une institution), ce dernier peut les utiliser ou les divulguer uniquement aux fins auxquelles l'institution était autorisée à les divulguer, ou selon ce qui est autorisé ou exigé par la loi, et doit aviser l'institution en cas d'atteinte à la vie privée.

Recommandation 21 : Amender l'annexe 2 par adjonction d'une disposition à la partie III de la LAIPVP imposant des restrictions aux destinataires tiers de renseignements personnels :

> ***XXX (1) Sauf selon ce qui est autorisé ou exigé par la loi et sous réserve des exceptions et exigences additionnelles, le cas échéant, qui sont prescrites, la personne à qui une institution divulgue des renseignements personnels et qui n'est pas elle-même une institution ne doit pas :***
>
> > ***a) utiliser ni divulguer les renseignements à d'autres fins que les fins auxquelles l'institution était autorisée à les divulguer en vertu de la présente loi ou l'exercice d'une obligation d'origine législative ou juridique;***
> > ***b) utiliser ni divulguer plus de renseignements qu'il n'est raisonnablement nécessaire pour réaliser les fins de l'utilisation ou de la divulgation, selon le cas.***
>
> ***(2) Si des renseignements personnels que l'institution a divulgués à un destinataire en vertu du paragraphe (1) sont soit volés ou perdus, soit utilisés ou divulgués sans autorisation, le destinataire avise l'institution qui lui a divulgué les renseignements personnels.***
>
> ***(3) L'avis mentionné au paragraphe (2) doit contenir les renseignements prescrits et être donné sous la forme ou de la manière prescrite dès que cela est faisable après que le destinataire a appris soit le vol ou la perte, soit l'utilisation ou la divulgation non autorisée.***

Les renseignements personnels concernant des enfants devraient être considérés comme étant de nature délicate

Nous félicitons le gouvernement de reconnaître la nécessité de protéger les renseignements personnels des enfants dans un monde de plus en plus numérique. Si le projet de loi 194 propose certains éléments permettant de renforcer ces protections dans l'annexe 1 (comme indiqué plus haut), il ne saisit pas l'occasion cruciale et opportune de le faire dans l'annexe 2 en modifiant la LAIPVP dans ce sens.

De plus en plus, les enfants et les jeunes sont exposés à la technologie numérique et se livrent quotidiennement à des activités en ligne, ce qui accroît le risque que leurs renseignements personnels soient utilisés de manière préjudiciable. Mon bureau a toujours demandé que l'on considère les renseignements personnels des enfants et des jeunes comme des renseignements de nature délicate qui nécessitent des mesures de précaution et de protection particulières.

Nous recommandons donc que l'annexe 2 contienne une disposition considérant les renseignements personnels des enfants et des jeunes comme des *renseignements personnels de nature délicate*. En outre, nous recommandons que l'obligation des institutions de procéder à des évaluations de l'impact sur la vie privée et de mettre en place les mesures de précaution d'ordre administratif et technique et les mesures de sécurité nécessaires soit modifiée en tenant compte du caractère plus délicat de ces renseignements.

Recommandation 22 : Amender l'annexe 2 du projet de loi 194 par adjonction d'un nouveau paragraphe 2 (5) à la LAIPVP selon lequel les renseignements personnels concernant des enfants et des jeunes seraient réputés être de nature délicate.

> ***2 (5) Dans la présente loi et les règlements, les renseignements personnels concernant des enfants et des jeunes sont réputés être de nature délicate.***

Recommandation 23 : Amender comme suit le paragraphe 4 (2) et l'article 5 de l'annexe 2 du projet de loi 194 qui proposent l'adjonction des nouveaux paragraphes 38 (3) et 40 (5) à la LAIPVP :

> *38 (3) Sauf disposition contraire des règlements, avant de recueillir des renseignements personnels, la personne responsable d'une institution veille à ce que soit préparée une évaluation écrite qui contient les renseignements suivants concernant les renseignements personnels que l'institution a l'intention de recueillir :*
>
> […]
>
> *8. Une explication des mesures de précaution d'ordre administratif, technique et matériel, ainsi que des pratiques qui seraient utilisées pour protéger les renseignements personnels conformément au paragraphe 40 (5) et un résumé des risques auxquels seraient exposés les particuliers en cas de vol ou de perte des renseignements personnels, ou de leur utilisation ou divulgation non autorisée**, en tenant compte de la nature délicate de ces renseignements**.*
>
> […]
>
> *40 (5) La personne responsable d'une institution prend les mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels dont l'institution a la garde ou le contrôle soient protégés contre le vol, la perte, et l'utilisation ou la divulgation non autorisée et pour veiller à ce que les documents dans lesquels sont consignés les renseignements personnels soient protégés contre la duplication, la modification ou l'élimination non autorisées**, en tenant compte de la nature délicate de ces renseignements**.*

Les dénonciateurs devraient être protégés contre des représailles éventuelles de leur employeur

L'annexe 2 du projet de loi 194 contient des dispositions importantes sur la dénonciation. Toute personne qui a des motifs raisonnables de croire qu'une institution a contrevenu à la LAIPVP ou est sur le point de le faire pourrait aviser mon bureau et demander que son identité demeure confidentielle. La mise en place d'un cadre législatif permettant aux employés du secteur public de dénoncer les actes répréhensibles, les risques ou la négligence correspond aux principes fondamentaux d'une loi moderne sur la protection de la vie privée et revêt une importance capitale pour garantir la gouvernance efficace des institutions.

Toutefois, dans certains cas, les employés peuvent hésiter à signaler des actes répréhensibles réels ou éventuels par crainte de représailles de la part de leur employeur. Dans son libellé

actuel, l'annexe 2 ne protège pas contre les représailles une personne qui a signalé (ou dont l'institution pense qu'elle signalera) une infraction au CIPVP. Dans bien des cas, l'institution pourra déduire l'identité de la personne, même si le commissaire ne la divulgue pas. Cette protection contre les représailles, qui est prévue à l'article 70 de la LPRPS et à l'article 330 de la LSEJF, est essentielle pour protéger le droit d'une personne à la dénonciation, tant du point de vue juridique que dans la pratique. Nous recommandons donc qu'une protection équivalente soit incluse dans la LAIPVP.

En outre, la possibilité d'informer le CIPVP et de demander que son identité reste confidentielle devrait être offerte aux dénonciateurs qui ont des préoccupations concernant toute personne qui a contrevenu à la LAIPVP ou est sur le point de le faire, et pas seulement les institutions et les services d'intégration des données.

Recommandation 24 : Amender l'article 10 de l'annexe 1 afin d'élargir les protections conférées aux dénonciateurs, et ajouter une disposition interdisant les représailles au paragraphe 57.1.

Dénonciation

57.1 (1) Toute personne qui a des motifs raisonnables de croire qu'une ~~institution, un service ministériel d'intégration des données visé à la partie III.1 ou un service multisectoriel d'intégration des données visé à la partie III.1~~ ***personne*** *a contrevenu à la présente loi ou aux règlements, ou est sur le point de le faire, peut aviser le commissaire des détails relatifs à la question et demander que son identité demeure confidentielle relativement à cette dénonciation.*

Caractère confidentiel
(2) Le commissaire est tenu de garder confidentielle l'identité de la personne qui l'a avisé en vertu du paragraphe (1) et à laquelle il a donné l'assurance de l'anonymat.

(3) Nul ne doit congédier, suspendre, rétrograder, punir ou harceler une personne ou lui faire subir tout autre désavantage pour l'un des motifs suivants :

a) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a divulgué au commissaire qu'une autre personne a contrevenu à une disposition de la présente loi ou de ses règlements ou est sur le point de faire;
b) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a accompli ou fait part de son intention d'accomplir tout acte nécessaire pour empêcher une personne de contrevenir à une disposition de la présente loi ou de ses règlements;
c) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a refusé d'accomplir ou fait part de son intention de refuser d'accomplir tout acte qui est en contravention à une disposition de la présente loi ou de ses règlements;
d) quelqu'un croit que la personne accomplira un des actes visés à l'alinéa a), b) ou c).

Le CIPVP recommande également d'amender l'annexe 2 du projet de loi 194 par adjonction d'une disposition correspondante au paragraphe 61 (1) de la LAIPVP en vertu de laquelle quiconque use de représailles contre un dénonciateur en contravention de l'interdiction précédente (semblable à celle qui existe déjà dans la LPRPS et la LSEJF) commet une infraction :

Recommandation 25 : Amender l'annexe 2 du projet de loi 194 par adjonction d'une nouvelle disposition à la LAIPVP en vertu de laquelle quiconque use de représailles contre un dénonciateur commet une infraction :

61 (1) Nul ne doit :
...
g) contrevenir au paragraphe 57.1 (3).

L'expansion des pouvoirs de ServiceOntario devrait être retirée de la LAIPVP

Le CIPVP est favorable à la modernisation des services gouvernementaux et à la mise en œuvre de technologies numériques pour rationaliser et améliorer la façon dont les Ontariennes et les Ontariens reçoivent ces services, pourvu que cela se fasse en toute sécurité et dans le respect du droit à la vie privée.

L'article 15 de l'annexe 2, si celle-ci était adoptée, modifierait l'article 65.1 de la LAIPVP de façon à élargir la définition de *renseignements liés au service à la clientèle* et permettrait à ServiceOntario de recueillir, d'utiliser et de conserver ces renseignements personnels supplémentaires. Il s'agit de renseignements personnels concernant les citoyens qui font appel à ServiceOntario pour obtenir et renouveler leur carte Santé, leur permis de conduire, leur carte-photo de l'Ontario et d'autres pièces d'identité essentielles. Ces nouveaux pouvoirs proposés seraient conférés à des fins qui vont au-delà de ce qui est prévu dans la loi habilitante de ServiceOntario et dans son règlement d'application, la *Loi sur le ministère des Services gouvernementaux* et le Règl. de l'Ontario 475/07.

La LAIPVP a pour principal objet de protéger les renseignements personnels des Ontariennes et des Ontariens que détient le gouvernement. Nous sommes préoccupés par le fait que le gouvernement propose d'utiliser la LAIPVP pour étendre considérablement la capacité de ServiceOntario à recueillir, utiliser et conserver des renseignements personnels dans le cadre d'un mode de prestation de services facultatif, sans avoir clairement démontré que ces pouvoirs supplémentaires sont nécessaires. En outre, le pouvoir de ServiceOntario de conserver et d'utiliser des renseignements personnels ne devrait pas être prévu dans la LAIPVP, qui est une loi sur la protection de la vie privée. Il serait plus approprié et plus transparent que l'expansion de tout pouvoir ou objet légal de ServiceOntario figure dans sa propre loi habilitante et son règlement d'application.

En outre, les modifications proposées à l'article 15 de l'annexe 2 élargiraient la définition des renseignements liés au service à la clientèle que ServiceOntario peut recueillir, utiliser et conserver, sans la protection correspondante d'un principe de minimisation des données. Conformément à la recommandation 15 plus haut, il est essentiel d'appliquer un tel principe afin de limiter la collecte et l'utilisation de renseignements personnels à une fin que d'autres renseignements peuvent réaliser et d'interdire la collecte et l'utilisation de plus de renseignements personnels qu'il n'est nécessaire pour réaliser la fin visée.

Recommandation 26 : Amender l'annexe 2 du projet de loi 194 par suppression de l'article 15. Si le gouvernement souhaite élargir les pouvoirs de ServiceOntario, il devrait le faire en modifiant la loi et le règlement habilitants de ServiceOntario au lieu d'apporter des modifications à la LAIPVP. Tout élargissement du pouvoir de ServiceOntario de recueillir des renseignements personnels concernant les Ontariennes et Ontariens, même en vertu de sa propre loi habilitante, devrait être circonscrit explicitement par un principe de minimisation des données afin d'éviter la création d'un registre central contenant les renseignements personnels que détient le gouvernement au sujet de la population.

Une disposition devrait être incluse prévoyant l'examen régulier de la loi pour s'assurer qu'elle demeure à jour

La LAIPVP est entrée en vigueur en 1988, il y a près de 40 ans, à une époque où les téléphones étaient encore essentiellement fixes, où les documents étaient presque exclusivement sur papier et où Google n'était qu'une vague idée. Depuis lors, les organisations ont considérablement changé la manière dont elles traitent les renseignements personnels, en raison des nombreuses technologies numériques qui sont désormais à leur disposition. Les nouvelles technologies se sont succédé à un rythme effréné, mettant à notre disposition des capacités de stockage numérique et une puissance de calcul considérables, l'Internet à haut débit, des appareils mobiles et des technologies prêt-à-porter, des plateformes de médias sociaux et, bien sûr, des systèmes d'intelligence artificielle.

Malgré ces changements profonds, la LAIPVP n'a jamais fait l'objet d'un examen approfondi jusqu'à présent. Pour éviter de nous retrouver dans la même situation à l'avenir, les lois et les politiques de l'Ontario ne peuvent pas demeurer en décalage par rapport à la technologie. Nous recommandons qu'une disposition soit ajoutée à la LAIPVP afin de garantir son examen régulier et son évolution au fil du temps pour qu'elle reste adaptée à la réalité moderne.

Recommandation 27 : Amender l'annexe 2 du projet de loi 194 afin de prévoir que l'Assemblée législative doit examiner la LAIPVP tous les cinq ans.

La LAIMPVP devrait faire l'objet de modifications équivalentes

Bien que mon bureau accueille favorablement les modifications apportées à la LAIPVP afin de la rapprocher des normes du XXI^{e} siècle, nous sommes préoccupés par le fait que le projet de loi 194 ne propose pas en même temps des modifications équivalentes à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP).

Modifier la LAIPVP mais pas la LAIMPVP perturberait considérablement l'harmonie, la cohérence et l'uniformité entourant la façon dont les renseignements personnels sont recueillis, utilisés, conservés et divulgués dans les institutions provinciales et municipales de l'Ontario. Ce décalage créerait une confusion et une incertitude inutiles pour les organisations du secteur public. Par ailleurs, les Ontariennes et Ontariens seraient déçus et se demanderaient pourquoi ils bénéficient de mesures différentes de protection de la vie privée selon qu'ils traitent avec la province ou, par exemple, leur ville, leur école ou leur bibliothèque publique.

En outre, l'établissement de règles claires concernant la déclaration des atteintes à la vie privée en vertu de la loi provinciale sur la protection de la vie privée, mais pas en vertu de son équivalent municipal, risque de brouiller les cartes à un moment critique où il faut informer les institutions de leurs nouvelles obligations. Les nouvelles attentes devront être parfaitement claires au moment de la mise en œuvre du projet de loi. Le fait de devoir expliquer quelles institutions publiques sont ou ne sont pas soumises à ces nouvelles dispositions compliquera inutilement les choses. Il n'est pas anodin de permettre aux institutions municipales de ne pas signaler les atteintes à la vie privée alors que les institutions provinciales sont tenues de le faire. Au cours des deux dernières années, deux tiers des atteintes à la vie privée et des plaintes signalées au CIPVP provenaient d'institutions assujetties à la LAIMPVP, et il ne s'agissait que de celles dont nous avons pris connaissance par le biais d'un régime de déclaration volontaire. Les municipalités et les institutions municipales telles que les écoles et les bibliothèques publiques continuent d'être d'importantes cibles de cyberattaques[30].

Réformer la LAIPVP sans apporter de modifications équivalentes à la LAIMPVP crée également une divergence dans les pouvoirs conférés au CIPVP pour faire enquête sur les atteintes à la vie privée. Cette situation compliquerait l'examen des cas où des institutions tant municipales que provinciales sont en cause, donnant lieu à des problèmes et à des retards importants. Nous serions moins en mesure d'examiner la circulation des données entre institutions. Ce serait le cas par exemple lors d'enquêtes sur des plaintes relatives à la protection de la vie privée faisant intervenir les réseaux de transport en commun de l'Ontario (à la fois Metrolinx et la Commission de transport de Toronto) ou les services policiers (à la fois la Police provinciale de l'Ontario et des services de police municipaux). C'est pourquoi nous recommandons vivement que des modifications équivalentes à celles que l'annexe 2 apporte à la LAIPVP soient également apportées à la LAIMPVP.

Recommandation 28 : Le CIPVP recommande vivement au gouvernement d'accélérer son projet d'instaurer des changements à la LAIMPVP qui sont équivalents à ceux qui sont apportés à la LAIPVP, afin que les Ontariennes et Ontariens jouissent de la même protection de leur vie privée auprès des institutions publiques provinciales et municipales.

Conclusion

Pour conclure, je tiens à réitérer notre appui au projet de loi 194, sous réserve des changements proposés plus haut. Mon bureau demeure résolu à collaborer avec le gouvernement et l'Assemblée législative pour renforcer le projet de loi actuel pour le bien de toute la population ontarienne.

Par souci d'ouverture et de transparence, la présente lettre et les pièces jointes seront publiées dans le site Web du CIPVP en anglais et en français.

---

[30] *Financial Post*. « Southern Ontario school board acknowledges 'cyber incident' », déc. 2023. Disponible à : https://financialpost.com/technology/southern-ontario-school-board-acknowledges-cyber-incident. *CBC*. « Hamilton library computers, other services remain down, 3 months after ransomware attack », mai 2024. Disponible à : https://www.cbc.ca/news/canada/hamilton/library-cyber-impact-continues-1.7203740.

Veuillez agréer, Madame, mes sincères salutations.

La commissaire,

Patricia Kosseim

c. c. Todd J. McCarthy, ministre des Services au public et aux entreprises et de l'Approvisionnement
Renu Kulendran, sous-ministre des Services au public et aux entreprises et de l'Approvisionnement
John Roberts, sous-ministre associé, ministère des Services au public et aux entreprises et de l'Approvisionnement
Melissa Kittmer, sous-ministre adjointe, ministère des Services au public et aux entreprises et de l'Approvisionnement
Mohammad Qureshi, directeur général de l'information pour la fonction publique, ministère des Services au public et aux entreprises et de l'Approvisionnement
Daniela Spagnolo, directrice générale de la sécurité de l'information, ministère des Services au public et aux entreprises et de l'Approvisionnement
Michelle Stock, chef de cabinet, ministère des Services au public et aux entreprises et de l'Approvisionnement

p. j.

ANNEXE

Recommandation 1 : Amender l'annexe 1 par adjonction de cette disposition d'objet [nota : le libellé proposé par le CIPVP figure en **caractères gras**] :

> ***[X] La présente loi a pour objet d'établir un cadre de gouvernance pour les entités du secteur public concernant les activités de cybersécurité, l'utilisation de systèmes d'intelligence artificielle et le déploiement de technologies numériques touchant les particuliers de moins de 18 ans, conformément aux principes suivants :***
>
> ***a) la vie privée des particuliers et des groupes doit être protégée, et il doit être interdit de recueillir, d'utiliser, de conserver et de divulguer plus de leurs renseignements personnels qu'il n'est nécessaire et proportionné pour réaliser la fin visée;***
>
> ***b) les entités du secteur public doivent remplir leurs obligations en vertu de la présente loi avec transparence dans la mesure où il est raisonnable et approprié de le faire, sans porter atteinte à la sécurité et à l'intégrité des systèmes d'information du gouvernement;***
>
> ***c) les systèmes d'intelligence artificielle doivent être valides, fiables et sûrs; ils doivent être conçus pour protéger la vie privée et affirmer les droits de la personne, et les entités du secteur public qui les utilisent doivent être responsables et transparentes;***
>
> ***d) les normes relatives aux technologies numériques touchant les personnes de moins de 18 ans doivent être élaborées et appliquées en tenant compte des droits des enfants et des jeunes et être conformes aux valeurs que sont l'autonomie personnelle, la dignité et l'autodétermination;***
>
> ***e) l'observation des dispositions de la présente loi et des règlements devrait être surveillée de façon indépendante du gouvernement.***

Recommandation 2 : Amender l'annexe 1 afin de reconnaître expressément le rôle et les fonctions du CIPVP en tant qu'organisme de surveillance indépendant par adjonction de la disposition suivante :

> ***[X] Le commissaire à l'information et à la protection de la vie privée exerce les fonctions et pouvoirs attribués par la* Loi sur l'accès à l'information et la protection de la vie privée, *la* Loi sur l'accès à l'information municipale et la protection de la vie privée, *la* Loi de 2004 sur la protection des renseignements personnels sur la santé, *la* Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille *et tout autre texte de loi qui lui attribue des pouvoirs et fonctions relativement aux entités du secteur public qui sont assujetties à la présente loi.***

Recommandation 3 : Amender l'annexe 1 pour prescrire un processus de consultation publique préalable à la prise de règlements en application de la loi. Cette exigence devrait s'inspirer de l'article 74 de la LPRPS.

Recommandation 4 : Amender l'annexe 1 afin que le ministre soit tenu de consulter le CIPVP avant de proposer ou de prendre un règlement ou de donner une directive pouvait se répercuter sur les droits des Ontariennes et Ontariens en matière d'accès à l'information et de protection de la vie privée. Cet amendement devrait s'inspirer des paragraphes 55.4 (2) et (3) de la LPRPS.

.

<u>Recommandation 5</u> : Amender l'annexe 1 pour exiger que les directives du ministre soient promulguées publiquement. Plus précisément, amender l'annexe 1 par adjonction des dispositions suivantes après les paragraphes 4 (3) et 11 (3) :

4 (X) Chaque directive donnée en vertu du paragraphe 4 (1) de la présente loi, à la fois :

- ***a) est mise à la disposition du public, sur demande;***
- ***b) est affichée publiquement sur au moins un site Web du gouvernement de l'Ontario.***

11 (X) Chaque directive donnée en vertu du paragraphe 11 (1) de la présente loi, à la fois :

- ***a) est mise à la disposition du public, sur demande;***
- ***b) est affichée publiquement sur au moins un site Web du gouvernement de l'Ontario.***

<u>Recommandation 6</u> : Amender l'annexe 1 pour protéger expressément les dénonciateurs.

Dénonciation
[X] (1) Quiconque a des motifs raisonnables de croire qu'une entité du secteur public ou toute autre personne a contrevenu à la présente loi, aux règlements ou à une directive aux termes de la présente loi ou est sur le point de le faire peut en aviser le commissaire ou un fonctionnaire désigné par le ministre et demander que son identité soit gardée confidentielle relativement à cette dénonciation.

Caractère confidentiel
(2) Le commissaire ou le fonctionnaire désigné par le ministre est tenu de garder confidentielle l'identité de la personne qui l'a avisé en vertu du paragraphe (1) et à laquelle il a donné l'assurance de l'anonymat.

Représailles interdites
(3) Nul ne doit congédier, suspendre, rétrograder, punir ou harceler une personne ou lui faire subir tout autre désavantage pour l'un des motifs suivants :

- ***a) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a divulgué au commissaire qu'une autre personne a contrevenu à une disposition de la présente loi ou des règlements ou à une directive ou est sur le point de faire;***
- ***b) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a accompli ou fait part de son intention d'accomplir tout acte nécessaire pour empêcher une personne de contrevenir à une disposition de la présente loi ou des règlements ou à une directive;***
- ***c) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a refusé d'accomplir ou fait part de son intention de refuser d'accomplir tout acte qui est en contravention à une disposition de la présente loi ou des règlements ou à une directive;***
- ***d) quelqu'un croit que la personne accomplira un des actes visés à l'alinéa a), b) ou c).***

Peine
(4) La personne qui enfreint le paragraphe (3) est coupable d'une infraction et est passible, sur déclaration de culpabilité, d'une amende d'au plus 5 000 $.

Recommandation 7 : Amender le paragraphe 2 (2) de l'annexe 1 afin que tout règlement sur les programmes de cybersécurité des entités du secteur public prévoie que tous les programmes comprennent certains éléments de base.

Règlements : programmes

(2) Sans préjudice de la portée générale de l'alinéa (1) b), un règlement pris en vertu de cet alinéa ~~peut~~ exige~~r~~ que le programme d'une entité du secteur public comprenne ce qui suit :

[…]
f) l'identification et la gestion de tout risque lié à la cybersécurité pour l'organisation, y compris les risques associés à la chaîne d'approvisionnement de l'entité du secteur public et à son recours à des produits et services externes;
g) des mesures visant à protéger contre toute attaque les systèmes informatiques de l'entité;
h) des processus visant à déceler les incidents liés à la cybersécurité qui portent ou peuvent porter atteinte aux systèmes informatiques d'une entité du secteur public;
i) des procédures visant à minimiser les répercussions des incidents liés à la cybersécurité.

Recommandation 8 : Amender l'annexe 1 pour enjoindre au ministre de fournir au CIPVP des copies des rapports qu'il reçoit d'institutions du secteur public en cas d'incident important lié à la cybersécurité qui fait ou pourrait faire intervenir des renseignements personnels.

[X] Le ministre fournit au commissaire à l'information et à la protection de la vie privée des copies des rapports qu'il reçoit de la part d'entités du secteur public en vertu de l'alinéa 2 (1) c), y compris des rapports élaborés par des tiers à la demande de ces entités, en ce qui concerne des incidents importants liés à la cybersécurité qui font ou pourraient faire intervenir des renseignements personnels.

Recommandation 9 : Amender l'annexe 1 afin d'enjoindre au ministre de produire un rapport annuel sur le nombre, les types et l'issue générale des cyberincidents signalés et sur les tendances qui se dégagent, et contenant d'autres renseignements pouvant être prescrits par règlement.

Recommandation 10 : Renforcer l'annexe 1 en codifiant des principes clairs qui serviront de balises encadrant l'utilisation responsable des systèmes d'IA par les entités du secteur public. La codification de ces balises, en plus de la disposition d'objet proposée dans la recommandation 1, fournirait les garanties nécessaires pour gagner et conserver la confiance des Ontariennes et des Ontariens dans l'utilisation des systèmes d'IA. Des précisions pourraient être apportées par le biais de règlements ou de normes techniques, ce qui permettrait d'adopter une approche réglementaire plus souple et plus évolutive.

Recommandation 11 : Modifier l'annexe 1 pour adopter explicitement un cadre fondé sur le risque. Ce cadre devrait évaluer l'incidence éventuelle et la probabilité des préjudices associés aux différents systèmes d'IA, en veillant à ce que les systèmes qui présentent un risque plus élevé de préjudice involontaire fassent l'objet d'une surveillance plus stricte que ceux qui sont classés comme présentant un risque moins élevé.

Recommandation 12 : Amender l'annexe 1 du projet de loi 194 afin d'y inclure une liste d'utilisations interdites des systèmes d'IA, qui pourrait être étoffée par règlement. Les utilisations interdites des technologies devraient être évaluées en fonction des principes fondamentaux de l'IA que le CIPVP propose dans la recommandation 10.

Recommandation 13 : Supprimer l'article 9 et l'alinéa 10 a) de l'annexe 1 et renforcer plutôt les dispositions relatives à la protection de la vie privée figurant dans la LAIPVP, la LAIMPVP et la partie X de la LSEJF afin de protéger les enfants et les jeunes dans le cadre d'un régime réglementaire de protection de la vie privée plus cohérent et homogène.

Recommandation 14 : Amender l'annexe 1 du projet de loi 194 afin que les directives et règlements du ministre sur les normes techniques concernant les technologies numériques mises à la disposition des particuliers âgés de moins de 18 ans s'appliquent à tous les fournisseurs de services au sens de la LSEJF ainsi qu'à toutes les autres institutions du secteur public dont on pourrait raisonnablement s'attendre à ce qu'elles mettent de pareilles technologies à la disposition des enfants et des jeunes.

Recommandation 15 : Amender l'annexe 2 en incluant dans la partie III de la LAIPVP un principe de minimisation des données semblable à celui qui existe déjà dans la LPRPS, la partie X de la LSEJF et la partie III.1 de la LAIPVP :

> ***XXX (1) Une institution ne doit pas recueillir, utiliser ou divulguer de renseignements personnels à une fin que d'autres renseignements permettent de réaliser.***
>
> ***(2) Une institution ne doit pas recueillir, utiliser ou divulguer plus de renseignements personnels qu'il n'est raisonnablement nécessaire pour réaliser la fin visée.***
>
> ***(3) Le présent article ne s'applique pas aux renseignements personnels que la loi oblige une institution à recueillir, à utiliser ou à divulguer.***

Recommandation 16 : Amender le paragraphe 4 (2) de l'annexe 2 (proposant d'ajouter de nouvelles dispositions à l'article 38 de la LAIPVP) pour circonscrire les situations où une institution peut recueillir des renseignements personnels concernant des Ontariennes ou des Ontariens avant d'avoir franchi les étapes requises pour minimiser les risques pour la vie privée qui ont été relevées dans une EIVP.

> *38 (4) La personne responsable d'une institution veille à ce que les mesures visées à la disposition 9 du paragraphe (3) soient mise* [sic] *en œuvre :*
>
> > *a) avant de recueillir les renseignements personnels visés à ce paragraphe,*
> > *b) dans un délai raisonnable après avoir recueilli les renseignements personnels, s'il est impossible de mettre en œuvre les mesures avant de les recueillir* ***et si les risques pour la vie privée des particuliers sont faibles****.*

Recommandation 17 : Amender le paragraphe 4 (2) de l'annexe 2 pour accroître le nombre de situations dans lesquelles les EIVP doivent être mis à jour en vertu du paragraphe 38 (5) proposé de la LAIPVP.

> *38 (5) Sauf disposition contraire des règlements, avant d'apporter toute modification importante aux ~~fins auxquelles les renseignements personnels visés~~ **renseignements énumérés** au paragraphe (3) ~~sont utilisés ou divulgués~~, la personne responsable d'une institution fait ce qui suit :*
>
> > *a) elle met à jour l'évaluation préparée en application du paragraphe (3) pour tenir compte de la modification proposée ~~et énoncer l'utilisation ou la divulgation prévue proposée~~;*
> > *b) elle met en œuvre les mesures supplémentaires déterminées en application de la disposition 9 du paragraphe (3).*

Recommandation 18 : Amender l'article 6 de l'annexe 2 afin d'élargir les motifs de plainte en matière de protection de la vie privée par adjonction du nouveau paragraphe 40.1 (4.1) à la LAIPVP et apporter un amendement corrélatif au nouveau paragraphe 40.1 (5) proposé de la LAIPVP.

> ***Plaintes en matière de protection de la vie privée***
>
> *40.1 **(4.1) Quiconque a des motifs raisonnables de croire qu'une autre personne a contrevenu à une disposition de la présente partie ou est sur le point de le faire peut porter plainte devant le commissaire.***

Délai de dépôt des plaintes

> *40.1 (5) Toute plainte visée au paragraphe (4**.1**) est faite par écrit et déposée auprès du commissaire au plus tard un an après que l'objet de la plainte a été porté pour la première fois à l'attention du plaignant ou après qu'il aurait dû raisonnablement être porté à son attention, selon le plus court de ces délais.*

Recommandation 19 : Amender l'article 7 de l'annexe 2 en élargissant la portée des pouvoirs d'enquête dont le commissaire a besoin pour effectuer les examens des pratiques relatives aux renseignements aux termes de l'article 49.0.1 proposé de la LAIPVP.

> *Examen par le commissaire des pratiques relatives aux renseignements*
> *49.0.1 (1) Le commissaire peut ~~examiner~~**déterminer la conformité d'une personne à la présente partie** ~~les pratiques relatives aux renseignements d'une institution~~ s'il a reçu une plainte aux termes du paragraphe 40.1 (4**.1**) ou qu'il a des motifs de croire qu'il n'est pas **ou ne sera pas** satisfait aux exigences de la présente partie.*
>
> *[…]*
>
> *Pouvoirs du commissaire*
> *(6) Le commissaire peut exiger la production de renseignements et de documents qui se rapportent à l'objet de l'examen ~~et qui sont sous la garde ou le contrôle d'une institution~~.*

Interrogatoire sous serment
(6.1) Le commissaire peut assigner à comparaître et interroger sous serment la personne qui, à son avis, pourrait avoir des renseignements relatifs à l'examen mené en vertu de la présente partie. Il peut faire prêter serment à cette fin.

Accès
(6.2) Lorsqu'il effectue un examen en vertu de la présente partie, le commissaire peut, à toute heure raisonnable et sans mandat ni ordonnance du tribunal, pénétrer dans un lieu autre qu'un logement pour effectuer une inspection afin de déterminer si les exigences en matière de sécurité y sont respectées.

Preuve
(6.3) Lorsqu'il effectue un examen en vertu de la présente partie, le commissaire peut recevoir et accepter les éléments de preuve et autres renseignements qu'il estime appropriés, qu'ils soient présentés sous serment, par affidavit ou autrement et qu'ils soient ou seraient admissibles ou non devant un tribunal judiciaire.

Ordonnances
(7) ~~*If, a*~~***A****près avoir donné à la personne responsable de l'institution* ***et à toute autre personne concernée*** *l'occasion d'être entendue****, le commissaire peut enjoindre à toute personne de s'acquitter d'une obligation imposée par la présente partie et, s'il*** *établit qu'une pratique relative aux renseignements contrevient à la présente partie, il peut ordonner à la personne responsable de prendre l'une ou l'autre des mesures suivantes :*

1. *Cesser la pratique relative aux renseignements.*
2. *Modifier la pratique relative aux renseignements, selon les indications du commissaire.*
3. *Retourner, transférer ou détruire les renseignements personnels recueillis ou conservés dans le cadre de la pratique relative aux renseignements.*
4. *Mettre en œuvre une pratique relative aux renseignements différente, selon les indications du commissaire.*
5. *Faire une recommandation concernant la façon dont la pratique relative aux renseignements pourrait être améliorée.*

Restriction applicable à certaines ordonnances
(8) Le commissaire ne peut ordonner, en vertu du paragraphe (5), que soient prises des mesures allant au-delà de ce qui est raisonnablement nécessaire pour se conformer à la présente partie.

Procédures
(9) La Loi sur l'exercice des compétences légales ne s'applique pas à un examen prévu ~~*au présent article*~~ ***à la présente partie****,* ***et le commissaire peut établir les règles de procédure qu'il estime nécessaires****.*

Recommandation 20 : Amender l'article 9 de l'annexe 2 pour éliminer toute ambiguïté concernant le fait que le commissaire peut communiquer les renseignements nécessaires à l'exercice de ses attributions en vertu du paragraphe 55 (1) de la LAIPVP.

55 (1) Le commissaire ou la personne qui agit pour son compte ou sous son autorité ne peuvent divulguer les renseignements portés à leur connaissance dans l'exercice de leurs attributions en vertu de la présente loi ou de toute autre loi, ***sauf si la divulgation est requise pour l'exercice de ces attributions ou*** *permise à une fin prescrite.*

Recommandation 21 : Amender l'annexe 2 par adjonction d'une disposition à la partie III de la LAIPVP imposant des restrictions aux destinataires tiers de renseignements personnels :

XXX (1) Sauf selon ce qui est autorisé ou exigé par la loi et sous réserve des exceptions et exigences additionnelles, le cas échéant, qui sont prescrites, la personne à qui une institution divulgue des renseignements personnels et qui n'est pas elle-même une institution ne doit pas :

a) utiliser ni divulguer les renseignements à d'autres fins que les fins auxquelles l'institution était autorisée à les divulguer en vertu de la présente loi ou l'exercice d'une obligation d'origine législative ou juridique;
b) utiliser ni divulguer plus de renseignements qu'il n'est raisonnablement nécessaire pour réaliser les fins de l'utilisation ou de la divulgation, selon le cas.

(2) Si des renseignements personnels que l'institution a divulgués à un destinataire en vertu du paragraphe (1) sont soit volés ou perdus, soit utilisés ou divulgués sans autorisation, le destinataire avise l'institution qui lui a divulgué les renseignements personnels.

(3) L'avis mentionné au paragraphe (2) doit contenir les renseignements prescrits et être donné sous la forme ou de la manière prescrite dès que cela est faisable après que le destinataire a appris soit le vol ou la perte, soit l'utilisation ou la divulgation non autorisée.

Recommandation 22 : Amender l'annexe 2 du projet de loi 194 par adjonction d'un nouveau paragraphe 2 (5) à la LAIPVP selon lequel les renseignements personnels concernant des enfants et des jeunes seraient réputés être de nature délicate :

2 (5) Dans la présente loi et les règlements, les renseignements personnels concernant des enfants et des jeunes sont réputés être de nature délicate.

Recommandation 23 : Amender comme suit le paragraphe 4 (2) et l'article 5 de l'annexe 2 du projet de loi 194 qui proposent l'adjonction des nouveaux paragraphes 38 (3) et 40 (5) à la LAIPVP :

38 (3) Sauf disposition contraire des règlements, avant de recueillir des renseignements personnels, la personne responsable d'une institution veille à ce que soit préparée une évaluation écrite qui contient les renseignements suivants concernant les renseignements personnels que l'institution a l'intention de recueillir :

[…]

8. Une explication des mesures de précaution d'ordre administratif, technique et matériel, ainsi que des pratiques qui seraient utilisées pour protéger les renseignements personnels conformément au paragraphe 40 (5) et un résumé des risques auxquels seraient exposés les particuliers en cas de vol ou de perte

*des renseignements personnels, ou de leur utilisation ou divulgation non autorisée**, en tenant compte de la nature délicate de ces renseignements**.*

[…]

*40 (5) La personne responsable d'une institution prend les mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels dont l'institution a la garde ou le contrôle soient protégés contre le vol, la perte, et l'utilisation ou la divulgation non autorisée et pour veiller à ce que les documents dans lesquels sont consignés les renseignements personnels soient protégés contre la duplication, la modification ou l'élimination non autorisées**, en tenant compte de la nature délicate de ces renseignements**.*

<u>Recommandation 24</u> : Amender l'article 10 de l'annexe 1 afin d'élargir les protections conférées aux dénonciateurs, et ajouter une disposition interdisant les représailles au paragraphe 57.1.

Dénonciation

57.1 (1) Toute personne qui a des motifs raisonnables de croire qu'une ~~institution, un service ministériel d'intégration des données visé à la partie III.1 ou un service multisectoriel d'intégration des données visé à la partie III.1~~ ***personne*** *a contrevenu à la présente loi ou aux règlements, ou est sur le point de le faire, peut aviser le commissaire des détails relatifs à la question et demander que son identité demeure confidentielle relativement à cette dénonciation.*

Caractère confidentiel

(2) Le commissaire est tenu de garder confidentielle l'identité de la personne qui l'a avisé en vertu du paragraphe (1) et à laquelle il a donné l'assurance de l'anonymat.

(3) Nul ne doit congédier, suspendre, rétrograder, punir ou harceler une personne ou lui faire subir tout autre désavantage pour l'un des motifs suivants :

a) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a divulgué au commissaire qu'une autre personne a contrevenu à une disposition de la présente loi ou de ses règlements ou est sur le point de faire;

b) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a accompli ou fait part de son intention d'accomplir tout acte nécessaire pour empêcher une personne de contrevenir à une disposition de la présente loi ou de ses règlements;

c) la personne, agissant de bonne foi et se fondant sur des motifs raisonnables, a refusé d'accomplir ou fait part de son intention de refuser d'accomplir tout acte qui est en contravention à une disposition de la présente loi ou de ses règlements;

d) quelqu'un croit que la personne accomplira un des actes visés à l'alinéa a), b) ou c).

Recommandation 25 : Amender l'annexe 2 du projet de loi 194 par adjonction d'une nouvelle disposition à la LAIPVP en vertu de laquelle quiconque use de représailles contre un dénonciateur commet une infraction :

> *61 (1) Nul ne doit :*
> ...
> ***g) contrevenir au paragraphe 57.1 (3).***

Recommandation 26 : Amender l'annexe 2 du projet de loi 194 par suppression de l'article 15. Si le gouvernement souhaite élargir les pouvoirs de ServiceOntario, il devrait le faire en modifiant la loi et le règlement habilitants de ServiceOntario au lieu d'apporter des modifications à la LAIPVP. Tout élargissement du pouvoir de ServiceOntario de recueillir des renseignements personnels concernant les Ontariennes et Ontariens, même en vertu de sa propre loi habilitante, devrait être circonscrit explicitement par un principe de minimisation des données afin d'éviter la création d'un registre central contenant les renseignements personnels que détient le gouvernement au sujet de la population.

Recommandation 27 : Amender l'annexe 2 du projet de loi 194 afin de prévoir que l'Assemblée législative doit examiner la LAIPVP tous les cinq ans.

Recommandation 28 : Le CIPVP recommande vivement au gouvernement d'accélérer son projet d'instaurer des changements à la LAIMPVP qui sont équivalents à ceux qui sont apportés à la LAIPVP, afin que les Ontariennes et Ontariens jouissent de la même protection de leur vie privée auprès des institutions publiques provinciales et municipales.