JUIN 2021

Observations du CIPVP dans le cadre des consultations du gouvernement de l'Ontario sur le *cadre de l'intelligence artificielle (IA) de confiance de l'Ontario*

Patricia Kosseim
Commissioner

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

Depuis deux ans, le gouvernement de l'Ontario (la « province ») sollicite des commentaires sur sa nouvelle approche concernant l'intelligence artificielle. Ainsi, il a mené en 2019 des consultations sur ce que l'on appelait à l'époque la Stratégie ontarienne relative aux données[1], il a publié en 2020 des « principes alpha » pour une utilisation éthique et la transparence dans le cadre de ses *Conseils sur l'intelligence artificielle (IA)*[2] et, plus récemment, il a mené des consultations sur *le cadre de l'intelligence artificielle (IA) de confiance de l'Ontario* (le « cadre »)[3].

Dans sa Stratégie ontarienne pour le numérique et les données[4] qu'elle a publiée récemment, la province annonce son intention de « bâtir une économie numérique alimentée par une IA éthique, ancrée dans les principes démocratiques et les droits individuels ». Cette stratégie est mentionnée dans la page Web relative aux consultations sur le cadre, lequel était présenté comme un élément fondamental à la mise en œuvre de la stratégie. Le cadre proposé s'articule autour de trois grands engagements provisoires, chacun étant assorti de trois mesures possibles. Les engagements provisoires sont les suivants :

1. **Aucune activité d'intelligence artificielle secrète :** L'utilisation que fait le gouvernement de l'IA doit toujours être transparente – les gens doivent savoir quand, pourquoi et comment les algorithmes sont utilisés et ils doivent connaître leurs droits en cas de préjudices.

2. **Une utilisation de l'IA en laquelle les Ontariens et Ontariennes peuvent avoir confiance :** Des règles et des outils sont en place pour utiliser de manière sécuritaire des algorithmes pour les programmes et les services gouvernementaux, tout en faisant une utilisation en fonction des risques.

3. **Une IA qui est au service de tous les Ontariens et Ontariennes :** La population ontarienne doit tirer des avantages économiques et sociaux des technologies d'IA – ces avantages doivent être arrimés aux droits individuels et reflètent les diverses communautés de la province.

Il s'agit là d'importants engagements pour la province; ils concordent généralement avec le mandat du Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) de protéger la vie privée et de favoriser la transparence. Conformément à notre priorité stratégique *La protection de la vie privée et la*

1 Gouvernement de l'Ontario. *Stratégie ontarienne relative aux données*, page Web mise à jour en janvier 2021, **https://www.ontario.ca/fr/document/strategie-ontarienne-relative-aux-donnees**.

2 Gouvernement de l'Ontario. *Conseils sur l'intelligence artificielle (IA)*, 30 mars 2021, **https://www.ontario.ca/fr/page/conseils-sur-lintelligence-artificielle-ia**.

3 Gouvernement de l'Ontario. *Consultations sur le cadre de l'intelligence artificielle (IA) de confiance de l'Ontario*, 5 mai 2021, **https://www.ontario.ca/fr/page/consultations-sur-le-cadre-de-lintelligence-artificielle-ia-de-confiance-de-lontario**.

4 Gouvernement de l'Ontario. *Créer un Ontario numérique*, 30 avril 2021, **https://www.ontario.ca/fr/page/creer-un-ontario-numerique.**

transparence dans un gouvernement moderne, nous avons pour objectif de défendre les droits des Ontariennes et des Ontariens en matière de protection de la vie privée et d'accès à l'information en collaborant avec les institutions publiques pour établir des principes fondamentaux et des cadres de gouvernance exhaustifs en vue du déploiement responsable de technologies numériques[5]. Dans le cadre d'un dialogue ouvert et permanent sur l'utilisation de l'IA en Ontario, nous exposons dans le présent document nos premières observations sur le recours à l'IA dans le secteur public dans le contexte des consultations de la province sur le cadre.

Nos observations comportent plusieurs considérations d'ordre général relatives à la structure et à la portée du cadre proposé. Nous abordons ensuite chaque engagement et proposons des éléments qui, à notre avis, renforceront les aspects du cadre qui portent sur l'accès à l'information et la protection de la vie privée. Nous sommes résolus à collaborer étroitement avec la province pour faire en sorte que les droits en matière de protection de la vie privée et d'accès à l'information soient au cœur du modèle provincial de gouvernance de l'IA.

CONSIDÉRATIONS D'ORDRE GÉNÉRAL

Le CIPVP soutient les engagements généraux proposés dans le cadre, qui devraient contribuer à tenir le gouvernement responsable de son utilisation de l'IA. Nous reconnaissons également que le cadre doit être étoffé et plus spécifique afin d'atteindre les résultats escomptés.

Étant donné la nature générale des engagements contenus dans le cadre, les commentaires suivants s'appuient sur notre propre expérience de l'IA et les technologies connexes ainsi que sur nos recherches à ce sujet. Ils soulignent également des aspects à approfondir à mesure que le gouvernement poursuit sa réflexion. Nous tenons à formuler des considérations générales au lieu d'énoncer des orientations ou propositions précises. Nous comptons sur un dialogue régulier avec la province au sujet du cadre.

1. DÉFINIR CLAIREMENT LES PRINCIPAUX CONCEPTS ENTOURANT L'IA ET LES CONCEPTS QUI SONT VISÉS PAR LE CADRE

Une définition de ce que sont l'IA et les concepts connexes doit compter parmi les éléments fondamentaux d'un modèle de gouvernance de l'IA. L'ambiguïté et

5 Commissaire à l'information et à la protection de la vie privée de l'Ontario. Priorités stratégiques du CIPVP 2021-2025, 22 avril 2021, **https://www.ipc.on.ca/about-us/priorites-strategiques-du-cipvp-2021-2025/?lang=fr.**

l'incompréhension susceptibles de résulter de l'absence de définitions précises pourraient donner lieu à des lacunes sur le plan de la responsabilisation et faire en sorte que des risques passent inaperçus. Une telle définition doit aussi être assez souple pour s'appliquer aux progrès technologiques futurs. Le cadre devrait donc comprendre des définitions claires des concepts clés liés à l'IA.

Voici une liste de définitions de certains éléments ou concepts clés concernant l'IA. Ces définitions visent à distinguer certains termes qui sont couramment utilisés de façon interchangeable. Leur but est d'éclaircir les commentaires qui suivent, mais nous participerions volontiers à toute initiative de la province visant à normaliser les définitions. Voici les principaux termes liés à l'IA :

- L'**intelligence artificielle** telle qu'elle est utilisée de nos jours recourt à l'informatique pour analyser certains types de données selon un modèle général du monde, afin d'atteindre des objectifs précis en générant des produits qui ont une incidence sur l'environnement externe[6]. L'IA n'est pas aujourd'hui, et ne sera pas dans un avenir prévisible, ce que l'on appelle dans la documentation scientifique une « intelligence artificielle générale », qui caractérise des machines capables de penser comme des êtres humains et dotées d'une conscience[7]. Les systèmes contemporains d'IA visent généralement à résoudre des problèmes précis et s'appuient sur une démarche particulière pour atteindre leurs objectifs. Les composantes de l'IA comprennent ce qui suit :
    - Un **modèle d'IA** est un ensemble d'instructions sur la façon d'interpréter un sujet donné, qui peut être établi explicitement par des êtres humains (l'IA classique) ou élaboré par apprentissage automatique. L'**apprentissage automatique** recourt à des démarches statistiques ou à d'autres démarches numériques pour constituer un modèle s'appuyant sur des **données d'apprentissage** d'une façon qui ne nécessite pas de programmation humaine en tant que telle. Les modèles peuvent être utilisés à diverses fins, notamment pour faire des **prévisions**, diviser les données en catégories par **classification**, et **générer** des données originales qui ressemblent à des exemples du monde réel.
    - Un **système d'IA** représente l'application d'un ou plusieurs modèles d'IA dans un système informatique implanté dans un environnement donné afin d'atteindre un objectif particulier. Ce système informatique peut nécessiter une intervention humaine, ou fonctionner de façon relativement autonome.

---

6 Cette définition s'appuie sur le modèle de définition d'IA présenté à la Commission européenne : *Proposal for a Regulation laying down harmonised rules on artificial intelligence*, Recital 6, 21 avril 2021, **https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.**

7 Voir p. ex. Santus, E., N. Christin, et H. Jayarm. « Artificial Intelligence », *Technology Factsheet Series,* Belfer Center for Science and International Affairs, Harvard Kennedy School, janvier 2020, **https://www.belfercenter.org/publication/technology-factsheet-artificial-intelligence**.

    - L'**environnement** dans lequel un système d'IA est implanté constitue un facteur clé. Cet environnement peut être observé par ce système (données saisies) et influencé sous l'action de ce système (produits). Un système d'IA peut fonctionner différemment en fonction de l'environnement.

- Un **algorithme** est un ensemble d'instructions élaboré en vue de résoudre un problème donné. Les algorithmes peuvent être intégrés dans un programme informatique, mais pas nécessairement. Ils sont utilisés en mathématiques, dans les tableurs et dans tous les aspects des logiciels, y compris pour l'IA. Il importe de distinguer les algorithmes de l'IA, car ils sont très répandus. Les modèles d'IA sont des exemples d'algorithmes (qui sont souvent très complexes). Ainsi, l'évaluation d'une demande de prestations gouvernementales en regard d'un ensemble de critères préétablis serait probablement considérée comme un algorithme, mais pas comme un système d'IA.

- Un **système décisionnel automatisé (SDA)** est défini dans la *Directive sur la prise de décisions automatisée* du gouvernement du Canada comme étant « toute technologie qui soit informe ou remplace le jugement des décideurs humains » et qui utilise des techniques comme celles employées dans les systèmes d'IA (y compris des méthodes statistiques et linguistiques)[8]. Certaines définitions précisent que les SDA ont incidence sur « les opportunités, l'accès, les libertés, les droits ou la sécurité »[9]. Il est important de distinguer les SDA de l'IA, car celle-ci peut être employée dans des contextes autres que la prise de décisions d'ordre administratif, où elle peut avoir moins d'incidence sur des particuliers ou groupes.

Le cadre devrait préciser s'il s'applique aux systèmes d'IA en général, ou uniquement à ceux qui répondent à une définition plus étroite de système décisionnel automatisé. Par exemple, s'appliquerait-il à un système d'IA qui n'analyse pas de renseignements sur des particuliers, ne prend pas de décisions à leur sujet, ni n'a d'incidence sur eux?

De même, la différence entre l'analyse statistique (une pratique de longue date du gouvernement) et l'IA n'est pas toujours évidente. Faute de portée bien définie (et compte tenu du fait que les termes « algorithme » et « IA » figurent dans le cadre), on ne sait trop si le cadre est censé s'appliquer à tous les processus du gouvernement qui sont axés sur des données, ou uniquement aux systèmes d'IA.

Nous ne prétendons pas qu'il existe une approche « correcte » quant à la portée des technologies couvertes par le cadre; il existe des arguments en faveur d'une application large (p. ex., les droits des particuliers concernant une décision devraient

8 Gouvernement du Canada. *Directive sur la prise de décisions automatisée*, modifié le 1er avril 2021, **https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592**.

9 Richardson, R. « Defining and Demystifying Automated Decision Systems », *Maryland Law Review* (à paraître), 26 mars 2021, **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811708**.

être essentiellement indépendants des technologies utilisées pour la prendre) ou d'une application étroite (p. ex., les cadres de gouvernance peuvent être plus spécifiques et ciblés lorsqu'ils sont appliqués à un ensemble plus restreint de processus). Cependant, quelle que soit la portée que l'on décide de donner au cadre, il importe que toutes les parties prenantes en fassent la même interprétation[10].

2. DÉFINIR CLAIREMENT LES INSTITUTIONS QUI SERONT ASSUJETTIES AU CADRE

L'IA, l'apprentissage automatique et la prise de décisions automatisée sont d'usage courant de nos jours. Un large éventail d'institutions mettent à l'essai ou implantent les technologies connexes à une variété de fins dans toute une série de programmes du secteur public provincial :

- **Soins de santé :** L'hôpital St. Michael de Toronto a mis en place un modèle d'apprentissage automatique qui analyse une vaste gamme de données, y compris les visites aux services des urgences, les conditions météorologiques et les événements prévus dans la région pour prévoir combien de patients se rendront aux services des urgences de l'hôpital un jour donné[11].
- **Services de police :** En Ontario, les forces de l'ordre envisagent le recours aux technologies de reconnaissance faciale qui s'appuie sur la vision par ordinateur, une technologie d'IA qui interprète des données visuelles et peut identifier et classer des objets en fonction d'images[12]. Le CIPVP s'intéresse activement à la question du recours à la reconnaissance faciale par la police dans le cadre de sa priorité stratégique *La nouvelle génération des forces de l'ordre.*
- **Éducation :** Certains examens universitaires qui ont lieu à distance sont surveillés par des logiciels qui recourent à l'apprentissage automatique pour déceler et prévoir les cas d'inconduite en milieu d'études. Par exemple, ces systèmes peuvent utiliser une variété de modèles d'IA qui classent en catégories des objets et activités en fonction de données recueillies par la surveillance en temps réel d'une variété de sources, comme l'utilisation de la souris et du

10 Remarque : Dans le présent document, par souci de clarté, nous mentionnons uniquement l'IA et les systèmes d'IA au lieu de recommander une portée particulière pour ce cadre.

11 Unity Health Toronto. *Strategic Plan 2019-2024*, 20 avril 2019; **http://bce.unityhealth.to/unity-health-toronto-strategic-plan-2019-2024.pdf**; Investissements Ontario. *Pleins feux : Un hôpital à Toronto prescrit l'IA pour réduire les temps d'attente aux urgences,* 10 février 2020, **https://www.investontario.ca/fr/pleins-feux/un-hopital-a-toronto-prescrit-lia-pour-reduire-les-temps-dattente-aux-urgences**.

12 Chellappa, R., P. Sinha, et P.J. Phillips. « Face Recognition by Computers and Humans », *IEEE Computer*, février 2009. **https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=903088**.

clavier de l'étudiant, des images captées par sa webcaméra et des sons perçus par les micros de son ordinateur[13].

- **Transport :** Le gouvernement de l'Ontario a collaboré avec des organismes en vue d'utiliser l'IA pour détecter le nombre de personnes à bord des véhicules qui empruntent les voies réservées aux véhicules multioccupants à accès spécial tarifé des routes de la province[14].
- **Prestation de services numériques :** Les propriétaires d'entreprises peuvent utiliser l'agent conversationnel « robotGO » pour obtenir des renseignements sur l'aide financière offerte par le gouvernement provincial[15]. Les agents conversationnels recourent souvent au traitement automatique du langage, un type d'IA conçu pour interpréter le langage et en produire et, parfois, générer un dialogue d'apparence réaliste avec des personnes.

De toute évidence, l'IA peut être employée de nombreuses façons, à des fins diverses et par des utilisateurs différents.

Compte tenu de l'utilisation généralisée de l'IA dans divers secteurs, le cadre devrait préciser les secteurs de programme ou les ministères qui seront soumis à ces engagements. Par exemple, la formulation d'une bonne partie du document de consultation donne à penser que l'accent est mis sur les systèmes d'IA qui sont destinés au public. Cependant, il faudrait également prendre en considération les systèmes d'IA qui peuvent être utilisés pour d'autres tâches d'arrière-plan, notamment l'élaboration de politiques, la planification et la prévision, et la cybersécurité. Ces activités se déroulent souvent hors de la vue du public, et dans certains cas, il peut être justifié de maintenir un certain degré de confidentialité (comme c'est le cas pour certaines mesures de cybersécurité).

3. S'ASSURER QUE LE CADRE S'APPLIQUE TOUT AU LONG DU CYCLE DE VIE DU SYSTÈME D'IA

Lorsqu'elle est mise en œuvre, l'IA, comme d'autres technologies, peut être considérée comme suivant un « cycle de vie » composé d'étapes distinctes : du concept initial à la

13 Graham, A. « As concerns linger, Western University promises solution to remote exam proctoring software », *Global News*, 14 mars 2021, **https://globalnews.ca/news/7693767/western-university-proctortrack-concerns/**

14 Gouvernement de l'Ontario. *Communiqué : L'Ontario améliore les services gouvernementaux en nouant des partenariats avec de petites entreprises*, 9 novembre 2017, **https://news.ontario.ca/fr/release/46968/lontario-ameliore-les-services-gouvernementaux-en-nouant-des-partenariats-avec-de-petites-entreprises.**

15 Gouvernement de l'Ontario. *Obtenir du financement du gouvernement de l'Ontario*, 14 février 2020. **https://www.ontario.ca/fr/page/obtenir-du-financement-du-gouvernement-de-lontario#section-4**

conception, puis la mise en œuvre, la transition vers la maintenance continue et enfin la mise hors service. Chaque étape de ce cycle de vie est marquée par des problèmes particuliers à résoudre, des mesures à prendre et des questions qui appellent une attention particulière.

Il peut être avantageux pour les institutions d'aborder l'IA de confiance sous l'angle du cycle de vie. Une telle approche peut contribuer à garantir que les risques pour l'accès à l'information, la protection de la vie privée et la confiance du public sont repérés et gérés au moment opportun. Un modèle de cycle de vie pour les systèmes d'IA proposé par l'Organisation de coopération et de développement économiques16 comprend les étapes suivantes :

1) **Conception, données et modèles** : Les objectifs du système, les principes sous-jacents, le contexte et le cahier des charges sont établis. Ensuite, les données sur lesquels s'appuiera le système d'IA sont recueillies, traitées et vérifiées. Les concepteurs créent ou sélectionnent un modèle ou algorithme qui est adapté ou entraîné en fonction de l'ensemble de données.

2) **Vérification et validation :** Les concepteurs évaluent le rendement de leur modèle en regard des objectifs, notamment en évaluant les faux positifs, les faux négatifs ou le rendement dans une variété de situations.

3) **Déploiement :** Le modèle et l'ensemble du système sont lancés dans un environnement donné. Le système peut commencer à surveiller l'environnement, évaluer les données recueillies au moyen de ses modèles et générer des produits comme des prévisions, des catégories, des décisions et des évaluations.

4) **Exploitation et suivi :** Le système d'IA est en exploitation, et ses produits sont utilisés en vue d'atteindre ses objectifs. Le système est surveillé en regard de critères de rendement et de qualité. Selon les résultats de cette surveillance, l'exploitant peut ramener le système à une étape antérieure afin d'en réévaluer la conception et l'entraînement.

Les institutions peuvent utiliser des systèmes d'IA à n'importe quelle étape du cycle de vie de ces systèmes. Ceux-ci peuvent être créés en interne, le produit d'un fournisseur peut être adapté aux spécifications du gouvernement, ou un secteur de programme peut s'abonner à un outil d'IA géré par un fournisseur et basé sur l'infonuagique. Quel que soit le moment où intervient une institution, il est important de prendre en compte chaque étape du cycle de vie, car les risques associés à l'IA sont présents à chacune d'entre elles.

16 Organisation de coopération et de développement économiques. « Paysage technique de l'IA », *L'intelligence artificielle dans la société*, 11 juin 2019. **https://www.oecd-ilibrary.org/sites/b7f8cd16-fr/index.html?itemId=/content/publication/b7f8cd16-fr**

Pour ces raisons, nous suggérons que le gouvernement précise que son cadre s'applique à toutes les étapes du cycle de vie des systèmes d'IA.

ENGAGEMENT 1 : AUCUNE ACTIVITÉ D'INTELLIGENCE ARTIFICIELLE SECRÈTE

L'utilisation que fait le gouvernement de l'IA doit toujours être transparente, juste et équitable.

Le CIPVP soutient fermement l'idée que le gouvernement divulgue ses utilisations de l'IA, conformément aux exigences relatives à la transparence de la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) et de son équivalent s'appliquant au secteur municipal, la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (*LAIMPVP*).

La *LAIPVP* et *LAIMPVP* s'appuient notamment sur le principe voulant que le fonctionnement ouvert et transparent des institutions démocratiques repose sur la possibilité d'être renseigné sur les activités du gouvernement. Comme l'a souligné la Cour suprême du Canada, les lois sur l'accès à l'information, qui peuvent aider le public à comprendre les activités du gouvernement, permettent à celui-ci d'être comptable de ces activités[17].

Cet engagement est important, car les systèmes d'IA peuvent remettre en cause la capacité du public à accéder aux informations sur les décisions et les activités du gouvernement de plusieurs manières. Par exemple, les modèles d'apprentissage automatique sont souvent si complexes qu'ils fonctionnent comme des « boîtes noires », c'est-à-dire que les données utilisées et évaluées, ainsi que le raisonnement qui sous-tend les décisions automatiques, ne sont pas faciles à comprendre ou à documenter[18].

Ce problème de transparence devient encore plus sérieux si une institution s'appuie sur des modèles créés par des organisations externes qui ne divulguent pas certaines de leurs particularités pour des raisons liées à la propriété intellectuelle[19], ou encore des modèles qui sont très intégrés au système et ne sont pas suffisamment

17 Cour suprême du Canada. *Dagg c. Canada*, 6 juin 1997, **https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/1525/index.do**.

18 Thomas, N., E. Chochia, et S. Linsday. *Regulating AI: Critical Issues and Choices*, Commission du droit de l'Ontario, avril 2021, **https://www.lco-cdo.org/wp-content/uploads/2021/04/LCO-Regulating-AI-Critical-Issues-and-Choices-Toronto-April-2021-1.pdf**.

19 Rubenstein, D. « Federal Procurement of Artificial Intelligence: Perils and Possibilities », *The Great Democracy Initiative*, **https://greatdemocracyinitiative.org/wp-content/uploads/2020/12/Artificial-Intelligence-Report_121320-FINAL.pdf**, p. 32.

documentés[20]. La difficulté d'expliquer le fonctionnement des systèmes d'IA peut compliquer la surveillance de la conformité de l'institution à ses obligations légales et autres, ce qui est particulièrement important à la lumière des préoccupations largement répandues concernant les biais et l'équité des systèmes d'IA.

Il est essentiel que les systèmes d'IA soient transparents pour gagner la confiance du public, et ce, pour diverses raisons, notamment parce que les préoccupations relatives aux effets discriminatoires des systèmes d'IA sur les communautés marginalisées sont bien documentées et de longue date. Les biais intégrés dans les modèles d'apprentissage automatique sont associés à des facteurs tels que les données utilisées pour les entraîner, les décisions prises par leurs créateurs au moment de leur conception et les critères utilisés pour évaluer et tester leur efficacité. La disparité entre le contexte dans lequel les données d'entraînement ont été recueillies et l'environnement dans lequel le système d'IA est déployé peut conduire à des déductions inexactes et à des décisions préjudiciables au sujet de particuliers et de communautés[21].

En vertu de la *LAIPVP*, l'institution doit prendre des mesures raisonnables pour veiller à ce que seuls soient utilisés les renseignements personnels consignés dans les documents dont elle a la garde et le contrôle qui sont exacts et à jour[22]. Les particuliers ont également le droit de demander la rectification des renseignements personnels qu'ils jugent inexacts et d'exiger qu'une déclaration de désaccord soit annexée aux renseignements personnels qui ne sont pas rectifiés[23]. Ces obligations et ces droits sont remis en question lorsque les décisions administratives qui sont prises à l'aide de systèmes d'IA ne sont pas facilement compréhensibles. Il est difficile pour un particulier de corriger les déductions biaisées ou discriminatoires qui sont faites à partir d'un modèle d'apprentissage automatique impénétrable. L'exactitude et la véracité sont des éléments clés du droit à la vie privée qui sont directement remis en question dans le contexte des systèmes d'IA.

---

20 Voir p. ex. Commissariat à la protection de la vie privée du Canada. *Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, la commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique*, 28 octobre 2020, **https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2020/lprpde-2020-004/.**

21 Voir p. ex. Buolamwini, J., et T. Gebru. « Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification », *Proceedings of Machine Learning Research*, vol. 81, p. 1-15, 2018, **http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.**

22 *Loi sur l'accès à l'information et la protection de la vie privée*, par. 40 (2), **https://www.ontario.ca/fr/lois/loi/90f31#BK62.** Une institution qui est dépositaire de renseignements sur la santé se voit imposer l'obligation semblable en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) de prendre des mesures raisonnables pour veiller à ce que les renseignements personnels sur la santé qu'elle utilise soient aussi exacts, complets et à jour que nécessaire compte tenu des fins auxquelles elle les utilise : *LPRPS*, par. 11 (1), **https://www.ontario.ca/fr/lois/loi/04p03#BK16**.

23 *Loi sur l'accès à l'information et la protection de la vie privée*, par. 47 (2), **https://www.ontario.ca/fr/lois/loi/90f31#BK72.** En vertu de la *LPRPS*, les particuliers ont un droit semblable de demander la rectification des renseignements personnels sur la santé qu'ils jugent inexacts, et d'exiger qu'une déclaration de désaccord soit annexée aux renseignements personnels sur la santé qui ne sont pas rectifiés : *LPRPS*, art. 55, **https://www.ontario.ca/laws/statute/04p03#BK77**.

4. JUSTIFIER LE SOUCI DE TRANSPARENCE POUR REMETTRE EN CAUSE NON SEULEMENT LES PRÉJUGÉS, MAIS ÉGALEMENT TOUTES LES INEXACTITUDES ET LA PERTINENCE GÉNÉRALE D'UN SYSTÈME D'IA

Deux des mesures possibles liées à l'engagement *Aucune activité d'intelligence artificielle secrète* consistent à être transparent lors de l'utilisation de l'IA pour prendre des décisions concernant des particuliers, et à permettre à ceux-ci de contester ces décisions si elles sont entachées de biais.

Soulignons que peu importe la source d'une erreur (biais ou autre), toute inexactitude devrait être contestable. Si les erreurs d'un système d'IA peuvent être le résultat d'un biais, elles peuvent aussi être la conséquence d'une inexactitude dans la mise en œuvre du système ou dans les données utilisées pour prendre une décision, ou encore d'une manière inappropriée d'aborder le problème. De même, le droit d'obtenir des explications ne vise pas uniquement à se protéger contre la partialité; il constitue un élément global de l'équité procédurale.

Au-delà de la possibilité offerte de contester des décisions individuelles, la transparence quant à l'utilisation des systèmes d'IA permet également aux particuliers de contester l'opportunité de certaines utilisations de l'IA. Dans certains cas, l'utilisation d'un système d'IA peut en soi avoir des répercussions importantes sur des populations ou des groupes de personnes (p. ex., en permettant une plus grande surveillance), même si les problèmes liés à l'exactitude et au biais dans des cas précis peuvent être résolus.

Nous demandons donc au gouvernement d'envisager de justifier la transparence non seulement pour lutter contre les biais, mais aussi en s'appuyant sur un éventail plus large de raisons pour lesquelles le public pourrait chercher à comprendre et, si nécessaire, à contester l'utilisation des systèmes d'IA et les résultats générés par ces systèmes.

5. ÉLARGIR LA PORTÉE DE SES ENGAGEMENTS EN MATIÈRE DE TRANSPARENCE

À notre avis, la troisième mesure possible associée au premier engagement (faire preuve de clarté et de transparence à l'égard du public quant à la façon dont l'Ontario recueille des données pour ses algorithmes) devrait être élargie pour faire en sorte que la population ontarienne puisse comprendre non seulement que des données sont recueillies, mais aussi *de quelles* données il s'agit.

Par exemple, les particuliers devraient avoir la possibilité d'examiner toute donnée recueillie en vue de son utilisation dans le cadre d'un processus décisionnel et de s'assurer de son exactitude. Comme indiqué ci-dessus, l'exactitude est un principe de protection de la vie privée qui, selon le CIPVP, devra jouer un rôle accru à l'ère de l'IA et de l'analytique des données.

Pour déterminer si un système d'IA donné est approprié, le particulier doit également savoir dans quel but il est utilisé et s'il atteint l'objectif visé. À cet effet, le cadre devrait inclure l'obligation de rendre publics les objets de chaque système d'IA et de développer des mécanismes permettant de démontrer publiquement l'efficacité d'un système dans la poursuite de ses objectifs.

Lorsque les faits démontrent que le système d'IA n'est plus efficace pour atteindre ses objectifs, les particuliers doivent être en mesure de contester son utilisation et d'en demander le retrait.

Pour conclure nos remarques concernant cet engagement, nous réitérons notre soutien à un mouvement général vers l'ouverture en ce qui concerne l'utilisation de l'IA par le gouvernement, mais nous soulignons que la transparence doit être comprise au sens large et englober l'ensemble du cycle de vie de l'IA. Cela inclut les raisons pour lesquelles l'IA est adoptée, la manière dont elle est élaborée, les données qu'elle utilise (à la fois lors de l'élaboration et pour des applications spécifiques), à quelles fins, la manière dont elle prend des décisions ou arrive à des résultats, la manière dont ces décisions sont mises en œuvre et l'efficacité avec laquelle elle atteint ses objectifs, etc. La connaissance de l'existence d'un système d'IA est une étape importante, mais ce n'est qu'une première étape.

6. METTRE PLUS L'ACCENT SUR LA RESPONSABILISATION

En octobre 2020, le CIPVP, de même que plusieurs autres organismes canadiens et internationaux de réglementation de la vie privée et de la protection des données, a parrainé une résolution portant sur la *responsabilisation dans le développement et l'utilisation de l'intelligence artificielle*[24] qui a été adoptée à l'Assemblée mondiale de la protection de la vie privée. Selon cette résolution, la responsabilisation est un élément crucial du développement légal et éthique de l'IA, et elle préconise d'évaluer les obligations de responsabilisation par rapport à des principes et des cadres clairement définis.

24 Assemblée mondiale de la protection de la vie privée. *Résolution sur la responsabilisation dans le développement et l'utilisation de l'intelligence artificielle*, 42e Assemblée mondiale de la protection de la vie privée, octobre 2020, **https://globalprivacyassembly.org/wp-content/uploads/2021/01/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-FR.pdf**.

La transparence est une composante essentielle d'un cadre global de responsabilisation des activités gouvernementales, mais la responsabilisation englobe bien plus que la transparence. Si l'on s'inspire de cette résolution internationale, la responsabilisation représente la démonstration du respect des lois, politiques et cadres en vigueur, « notamment par l'adoption et la mise en œuvre de mesures appropriées, réalisables, systématiques et efficaces »[25].

Ainsi, bien que le premier engagement du cadre fasse référence de manière indirecte au concept de responsabilisation, nous invitons le gouvernement à mettre davantage l'accent sur ce principe clé en l'élevant au rang d'engagement autonome. À l'appui d'un tel engagement, plusieurs mesures possibles seraient nécessaires pour établir les composantes de base d'un programme de responsabilisation efficace, notamment :

- **Élaborer une structure de gouvernance interne claire pour l'IA.** Une structure de gouvernance interne devrait définir des rôles et des responsabilités clairs et documenter les décisions de gestion essentielles relatives à l'utilisation de l'IA conformément au cadre, comme l'approbation des évaluations des risques, l'approbation des points où le processus décisionnel nécessite l'intervention humaine et l'approbation des politiques et des procédures à l'appui du cadre et de ses engagements.
- **Nomination d'une personne responsable de la supervision de l'IA**. Cette personne superviserait l'adhésion d'une institution au cadre, aiderait à développer des ressources et des procédures, agirait en tant que promoteur interne du cadre et serait accessible au public pour toute question concernant les pratiques d'IA de l'institution.
- Établir des normes d**'engagement et de consultation.** Les responsables de la mise en œuvre de l'IA devraient également comprendre les limites de leur propre expertise et établir des critères pour déterminer quand faire appel à d'autres parties pour déterminer les mesures de responsabilisation nécessaires. Par exemple, au cours de la conception, le gouvernement provincial devrait tenir compte de la suggestion du Centre for Information Policy Leadership selon laquelle les concepteurs de systèmes devraient consulter des conseils d'examen internes ou externes pour obtenir une orientation sur les systèmes à risque élevé[26].

---

25 *Ibid*. Voir aussi des définitions semblables dans : Centre for Information Policy Leadership. *What Good and Effective Data Privacy Accountability Looks Like*, mai 2020, **https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report__27_may_2020__v2.0.pdf**, et Information Accountability Foundation. *The Essential Elements of Accountability*, janvier 2019, **https://informationaccountability.org/publications/**.

26 Centre for Information Policy Leadership. *CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU*, 22 mars 2021, **https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_risk-based_approach_to_regulating_ai__22_march_2021_.pdf**.

- **Établir des mécanismes de dénonciation ou de signalement.** Ces mécanismes constitueraient un moyen clair de signaler sans crainte de représailles les cas de non-respect de la loi, d'utilisation non autorisée à risque élevé de l'IA ou de non-respect du cadre.

Nous recommandons donc au gouvernement d'exiger des contrôles de gestion appropriés pour surveiller la conformité au cadre, par le biais d'un engagement supplémentaire visant à garantir la responsabilisation en ce qui concerne l'utilisation responsable de l'IA, ainsi que les mesures possibles connexes nécessaires à sa mise en œuvre efficace.

ENGAGEMENT 2 : UNE UTILISATION DE L'IA EN LAQUELLE LES ONTARIENS ET ONTARIENNES PEUVENT AVOIR CONFIANCE

Des règles fondées sur des risques sont en place pour assurer l'utilisation sécuritaire et équitable de l'IA par le gouvernement.

Les autorités chargées de la protection de la vie privée et des données, y compris le CIPVP, reconnaissent que l'IA représente un risque fondamental pour de nombreux principes sur lesquels repose la législation relative à la protection de la vie privée[27]. Par exemple, l'IA, et particulièrement l'apprentissage automatique, remettent en question le principe consistant à *limiter la collecte de renseignements*, car les modèles d'IA, en règle générale, fonctionnent le mieux lorsqu'ils sont alimentés par de grandes quantités de données variées. Il n'est pas rare non plus que des organisations réaffectent des données déjà recueillies pour les utiliser dans le cadre de l'entraînement de l'IA, remettant en cause le principe selon lequel *les données doivent être utilisées uniquement aux fins prévues*[28]. L'idée de *limiter la conservation des données* est incompatible avec l'apprentissage automatique, car les données utilisées lors de l'entraînement et les informations qui en découlent peuvent persister dans un modèle

27 Conférence internationale des commissaires à la protection des données et de la vie privée. « Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle », *40e Conférence internationale des commissaires à la protection des données et de la vie privée*, 23 octobre 2018. **http://globalprivacyassembly.org/wp-content/uploads/2018/10/20181023_ICDPPC-Declaration-AI_Adopted-FR.pdf**; Résolution des commissaires fédéral, provinciaux et territoriaux à l'information et à la protection de la vie privée : *Pour une législation efficace sur la protection des renseignements personnels et l'accès à l'information dans une société guidée par les données*, 1er et 2 octobre 2019, **https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_191001/**.

28 Centre for Information Policy Leadership. « First Report: Artificial Intelligence and Data Protection in Tension. Artificial Intelligence and Data Protection », *Delivering Sustainable AI Accountability in Practice*, 10 octobre 2018, **https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf**.

longtemps après que les données d'entraînement sous-jacentes ont été supprimées ou sont devenues périmées[29].

En outre, l'anonymisation, l'un des fondements du partage des données dans le respect de la vie privée, est remise en question par des recherches montrant que les modèles d'apprentissage automatique peuvent parvenir à désanonymiser de grandes parties d'ensembles de données que l'on croyait anonymisées[30].

Ces remises en question des pratiques exemplaires actuelles en matière de protection de la vie privée soulignent l'importance de faire preuve de diligence raisonnable à l'égard des systèmes d'IA susceptibles d'utiliser des renseignements personnels. Le CIPVP soutient l'engagement proposé par le gouvernement d'adopter une approche fondée sur le risque pour l'utilisation de l'IA, et les considérations que nous avançons ont pour but de préciser comment cet engagement peut être renforcé. Nous sommes également en faveur de tests qui examinent la robustesse, la fiabilité, l'exactitude et la sécurité des systèmes d'IA, y compris l'identification et la correction des biais dans les systèmes.

Selon la *r*ésolution sur la responsabilisation dans le développement et l'*utilisation de l'intelligence artificielle* de l'Assemblée mondiale de la protection de la vie privée que nous avons parrainée en 2020, le CIPVP s'est engagé à travailler de concert avec des organisations pour évaluer les risques pour les droits en matière de protection de la vie privée et d'accès à l'information ainsi que d'autres droits de la personne avant que des systèmes d'IA soient implantés[31]. Notre travail dans ce domaine s'aligne également sur notre priorité stratégique *La protection de la vie privée et la transparence dans un gouvernement moderne*.

---

29 Izzo, Z. et coll. « Approximate Data Deletion from Machine Learning Models », *Proceedings of the 24th International Conference on Artificial Intelligence and Statistics (AISTATS) 2021*, à paraître, **https://arxiv.org/abs/2002.10077**.

30 Rocher, L., J.M. Hendrickx, et Y. de Montjoye. « Estimating the success of re-identifications in incomplete datasets using generative models », *Nature Communications*, vol. 10, n° 3069, 2019. **https://www.nature.com/articles/s41467-019-10933-3**

31 Voir les paragraphes 1 (1) et (2), Assemblée mondiale de la protection de la vie privée. *Résolution sur la responsabilisation dans le développement et l'utilisation de l'intelligence artificielle*, 42e Assemblée mondiale de la protection de la vie privée, octobre 2020, **https://globalprivacyassembly.org/wp-content/uploads/2021/01/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-FR.pdf**.

7. DÉFINIR UNE PORTÉE, DES CRITÈRES ET UNE MÉTHODOLOGIE CLAIRS POUR L'ÉVALUATION DES RISQUES ET PUBLIER LES RÉSULTATS DES ÉVALUATIONS

En ce qui concerne la mesure possible consistant à « décider s'il faut utiliser un outil d'évaluation de l'algorithme pour mesurer les risques, la sécurité et la qualité », nous constatons que de nombreuses formes d'évaluation peuvent se révéler nécessaires en fonction des différentes catégories de risques. De nombreux outils existants d'évaluation de l'incidence algorithmique sont axés principalement sur les systèmes décisionnels automatisés et se concentrent essentiellement sur la possibilité d'expliquer et de vérifier le système, ainsi que sur l'équité de ce dernier[32]. Il s'agit là d'aspects essentiels en regard desquels les systèmes décisionnels automatisés devraient être évalués, et nous invitons le gouvernement à tirer profit des méthodologies existantes d'évaluation de l'incidence algorithmique. Cependant, nous aimerions aussi nous assurer que les outils existants d'évaluation du risque pour la vie privée soient également utilisés dans les cas pertinents.

Nous constatons que l'outil d'évaluation de l'incidence algorithmique (EIA) du gouvernement du Canada[33] souligne que si des renseignements personnels sont utilisés, une évaluation de l'incidence sur la vie privée pourrait devoir être effectuée en plus d'une EIA. De même, l'évaluation de l'incidence algorithmique n'évalue pas la cybersécurité à un niveau que le permettraient les méthodologies établies d'évaluation des menaces et des risques et les tests d'intrusion.

Nous revenons également sur nos considérations précédentes 1 et 3, et soulignons que des définitions claires et une approche basée sur le cycle de vie seront essentielles pour élaborer un processus permettant de déterminer les types de systèmes qui devront être évalués en fonction des risques, et à quel moment du cycle de vie ces évaluations devront avoir lieu. Des définitions claires revêtent également de l'importance pour attribuer des niveaux de risque de manière cohérente.

Le cadre devrait préciser si une approche fondée sur le risque doit être appliquée à toutes les utilisations de l'IA, qu'elles comportent ou non le traitement de renseignements personnels, en reconnaissant le risque que l'utilisation de systèmes d'IA puisse désanonymiser des renseignements que l'on croyait auparavant anonymisés.

32 Reisman, D. et coll. *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, AI Now Institute, New York University, 2018, **https://ainowinstitute.org/aiareport2018.pdf**.

33 Gouvernement du Canada. Évaluation de l'*incidence algorithmique*, modifié le 22 mars 2021, **https://open.canada.ca/aia-eia-js/?lang=fr**.

Conformément à l'engagement *Aucune d'activité d'IA secrète* et à la *Directive sur la prise de décisions automatisée*[34] du gouvernement du Canada, nous tenons également à rappeler à la province l'importance de consigner les évaluations des risques qu'elle effectue et nous l'encourageons à publier les rapports d'évaluation, ou du moins des résumés, dans la mesure du possible.

8. ÉLABORER DES MÉCANISMES POUR GARANTIR QUE L'OBJET D'UN SYSTÈME D'IA N'EST PAS MODIFIÉ DE MANIÈRE IMPORTANTE SANS RÉÉVALUATION

La plupart des évaluations des risques sont des analyses « ponctuelles », ce qui signifie que les objectifs, la conception, ainsi que les politiques et procédures connexes du système et d'autres informations sont examinés pour y déceler des risques et qu'un rapport contenant des recommandations sur la manière d'atténuer ces risques est publié. Les évaluations des risques sont souvent périmées ou caduques lorsqu'un système change ou que de nouvelles utilisations sont adoptées.

Par exemple, une évaluation des risques d'un système de reconnaissance faciale utilisé par les forces de l'ordre dans des installations à haute sécurité peut être effectuée, et des mesures d'atténuation appropriées à ce contexte peuvent être mises en place. Toutefois, si les forces de l'ordre devaient étendre l'utilisation des systèmes de reconnaissance faciale au-delà des installations à haute sécurité pour permettre une surveillance plus générale dans de nouvelles catégories d'installations, les risques pourraient augmenter ou de nouveaux risques pourraient être introduits.

C'est pourquoi nous appuyons la proposition de la province de vérifier continuellement les biais et les risques, et nous suggérons qu'elle envisage de mettre en place des mécanismes permettant de déclencher la tenue de réévaluations si certains critères changent, par exemple lorsque l'utilisation réelle diffère de l'utilisation prévue à l'origine, ou si l'efficacité du système est réduite (conformément à notre considération 4).

34 Gouvernement du Canada. *Directive sur la prise de décisions automatisée*, modifié le 1er avril 2021, annexe C, **https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592**.

9. VEILLER À METTRE EN PLACE LES CRITÈRES, LE FINANCEMENT, LA FORMATION, LES STRUCTURES INSTITUTIONNELLES ET LES AUTRES SOUTIENS NÉCESSAIRES À LA SURVEILLANCE ET À L'INTERVENTION HUMAINES REQUISES

La surveillance humaine peut jouer un rôle important pour maintenir la confiance dans l'IA. Nous soutenons fermement une approche basée sur les risques pour déterminer quand une surveillance et une intervention humaines s'imposent dans un système d'IA. Nous soulignons également que cette surveillance et cette intervention jouent un rôle tout au long du cycle de vie des systèmes d'IA.

Selon la *Directive sur la prise de décisions automatisée* du gouvernement du Canada, pendant le fonctionnement normal d'un système décisionnel automatisé, les systèmes à risque élevé ne peuvent prendre de décision sans qu'il y ait des points d'intervention humaine précis pendant le processus décisionnel, et la décision définitive doit être prise par un humain. Dans la foulée de cette recommandation, la directive prévoit également la formation des employés afin qu'ils soient en mesure « d'examiner, d'expliquer et de surveiller » le fonctionnement d'un système décisionnel automatisé[35].

Le gouvernement provincial devrait appliquer des critères clairs quant aux situations où sont requises la surveillance et l'intervention humaines dans les systèmes, et s'assurer que le financement, la formation, les structures institutionnelles et d'autres soutiens sont en place pour garantir l'efficacité de cette surveillance et de cette intervention.

10. CLARIFIER L'ALIGNEMENT ENTRE LA STRATÉGIE D'IA D'UNE PART ET LES CADRES LÉGISLATIFS CONNEXES ET RÉFORMES PROPOSÉES D'AUTRE PART

On reconnaît la nécessité de mettre à jour les lois canadiennes sur la protection de la vie privée afin d'éliminer les obstacles à l'innovation et de combler les lacunes en matière de protection qui sont apparus à la suite des progrès technologiques des deux dernières décennies[36].

En ce qui concerne les initiatives récentes relatives à la surveillance législative de l'IA, soulignons que les modifications récentes apportées à la *LAIPVP* ont créé un cadre

35 Gouvernement du Canada. *Directive sur la prise de décisions automatisée*, modifié le 1er avril 2021, paragraphe 6.3.5, **https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592**.

36 Voir p. ex. Scassa, T. « Data Protection Law », *Artificial Intelligence and the Law in Canada* (F. Martin-Bariteau et T. Scassa, *éd.*), LexisNexis, 2021.

pour le partage de renseignements personnels entre les ministères (et avec les services extraministériels d'intégration des données) à certaines fins désignées. La mesure dans laquelle il est prévu d'utiliser l'IA dans les services d'intégration des données n'est pas encore claire à l'heure actuelle.

La province étudie également la possibilité d'adopter une loi sur la protection de la vie privée dans le secteur privé. Une approche harmonisée de la protection des droits en matière de protection de la vie privée (y compris l'accès à ses propres renseignements personnels et l'explication des décisions qui les concernent) dans le contexte de la prise de décisions automatisée dans les secteurs public et privé contribuerait à la cohérence et à l'uniformité du cycle de vie des systèmes d'IA, qui peut faire intervenir des entités commerciales à diverses étapes.

Le gouvernement devrait préciser comment sa stratégie en matière d'IA s'aligne sur les lois existantes et nouvelles. Nous formulerions volontiers des conseils sur la manière de parvenir à un tel alignement et à une telle cohérence réglementaire.

ENGAGEMENT 3 : UNE IA QUI EST AU SERVICE DE TOUS LES ONTARIENS ET ONTARIENNES

Le gouvernement utilise l'IA d'une manière qui reflète et protège les droits et valeurs de la population ontarienne.

Comme nous l'avons évoqué, le CIPVP reconnaît que les systèmes d'IA peuvent avoir de nombreuses répercussions sur les droits de la personne. Nous nous sommes concentrés en particulier sur les questions d'accès à l'information et de protection de la vie privée, conformément à notre mandat. Cependant, comme nous l'avons vu plus haut, certaines questions liées à l'utilisation de l'IA, et en particulier les biais, la discrimination et l'équité, dépassent le mandat du CIPVP et touchent d'autres aspects des droits de la personne. Les préoccupations éthiques soulevées lorsque les gouvernements confient à des mandataires artificiels des décisions prises normalement par des êtres humains doivent être examinées attentivement. Le gouvernement provincial aurait avantage à consulter la Commission ontarienne des droits de la personne, l'Ombudsman de l'Ontario et des spécialistes de l'éthique à ce sujet.

Dans cette optique, les considérations que nous proposons à l'égard de l'engagement *Une IA qui est au service de tous les Ontariens et Ontariennes* visent à s'assurer que la province 1) met en œuvre des critères clairs en ce qui concerne les systèmes d'IA posant des risques inacceptables; 2) attribue soigneusement et de façon coordonnée les fonctions de surveillance aux différents organismes existants, le cas échéant; 3) reconnaît l'applicabilité de nombreuses orientations et démarches de gouvernance déjà existantes à certains aspects des systèmes d'IA; et 4) examine attentivement ce

que signifie vraiment être au service de tous les Ontariens et Ontariennes et tienne des consultations à ce sujet.

11. ENVISAGER D'ÉLARGIR LES CRITÈRES SELON LESQUELS CERTAINES UTILISATIONS DE L'IA SONT INTERDITES, AU MOINS TEMPORAIREMENT

De nombreuses initiatives sont en cours pour interdire ou limiter considérablement l'utilisation de l'IA dans certains contextes. Par exemple, le règlement récemment proposé par l'Union européenne crée une catégorie de systèmes d'IA « à risque élevé », qui sont soumis à des exigences plus strictes que les autres systèmes. Ce règlement interdit aussi strictement les pratiques d'IA qui vont à l'encontre des valeurs de l'UE (p. ex., parce qu'elles violent les droits de la personne) et présentent donc un « risque inacceptable »[37]. Par ailleurs, en 2019, l'État de Californie a interdit le recours à la reconnaissance faciale avec les caméras d'intervention des services de police[38] pour une période de trois ans, pour donner le temps de mettre en place des mesures de précaution supplémentaires liées à l'utilisation de la technologie[39].

Nous sommes donc heureux qu'une des mesures possibles soit de déterminer si le gouvernement devrait interdire l'utilisation de l'IA dans certaines situations, lorsque les populations vulnérables courent un risque extrêmement élevé. Toutefois, nous invitons la province à se demander s'il n'y aurait pas d'autres situations dans lesquelles l'utilisation de l'IA serait inappropriée, par exemple si l'on risquait de porter atteinte aux droits de la personne de la population ontarienne en général.

Nous aimerions également attirer votre attention sur le document d'orientation *Ethics, Transparency and Accountability Framework for Automated Decision-Making*[40] publié récemment par l'Office for Artificial Intelligence du gouvernement du Royaume-Uni. Il propose la considération suivante :

---

37 Commission européenne. *Proposal for a Regulation laying down harmonised rules on artificial intelligence*, 21 avril 2021, **https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence**.

38 Electronic Privacy Information Center. *State Facial Recognition Policy*, **https://epic.org/state-policy/facialrecognition/**.

39 Thebault, R. « California could become the largest state to ban facial recognition in body cameras », *The Washington Post*, 11 septembre 2019, **https://www.washingtonpost.com/technology/2019/09/12/california-could-become-largest-state-ban-facial-recognition-body-cameras/**.

40 Gouvernement du Royaume-Uni. *Guidance: Ethics, Transparency and Accountability Framework for Automated Decision-Making*, 13 mai 2021, **https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making**.

[Traduction]

Avant d'utiliser ce cadre, il faut se demander si l'utilisation d'un système automatisé ou algorithmique est appropriée dans les circonstances.

Toutes les décisions automatisées et algorithmiques doivent être examinées avec soin. Elles ne doivent pas être la solution privilégiée pour résoudre les questions les plus complexes et les plus difficiles en raison du risque élevé qui leur est associé.

La province devrait inclure un énoncé de cette nature dans son cadre. Un engagement de faire preuve de prudence à l'égard des applications d'IA à risque élevé, surtout en l'absence d'exigences législatives, de mécanismes de surveillance ou de contrôles techniques solides, contribuerait à assurer la confiance dans la stratégie d'IA de la province.

12. CONCEVOIR AVEC SOIN DES MÉCANISMES DE SURVEILLANCE INDÉPENDANTE

Une surveillance forte et indépendante devrait être un élément clé du cadre. Elle doit inclure à la fois la capacité d'effectuer des vérifications et des examens proactifs du fonctionnement des systèmes d'IA[41] et offrir une voie de recours aux personnes souhaitant contester les résultats des systèmes d'IA. Le fardeau de contester les résultats individuels des systèmes d'IA et de déceler les biais systémiques plus larges au sein de ces systèmes ne devrait pas reposer entièrement sur les particuliers concernés. Dans son rapport *Réglementer l'intelligence artificielle – Enjeux et choix essentiels*, la Commission du droit de l'Ontario (CDO) a donné son appui au principe de la surveillance indépendante de l'IA et des systèmes décisionnels automatisés au sein du gouvernement, mais a dit hésiter quant à la nature de ces fonctions de surveillance et aux points où elles seraient exercées[42].

Le CIPVP serait heureux de pouvoir collaborer avec le gouvernement et d'autres parties prenantes (telles que le CDO) afin d'élaborer un modèle de surveillance indépendante adapté aux besoins. Ce modèle devrait être élaboré avec soin, de concert avec les organismes de surveillance déjà en place, tels que le CIPVP, la

41 Commissariat à la protection de la vie privée du Canada. *Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE*, novembre 2020, **https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/**.

42 Thomas, N., E. Chochia, et S. Linsday. *Réglementer l'intelligence artificielle – Enjeux et choix essentiels* (sommaire), Commission du droit de l'Ontario, avril 2021, **https://www.lco-cdo.org/wp-content/uploads/2021/04/CDO-Reglementer-lintelligence-artificielle-Enjeux-et-choix-essentiels-Sommaire-Toronto-avril-2021.pdf.**

Commission ontarienne des droits de la personne, l'Ombudsman ainsi que l'autorité en matière de données récemment proposée[43]. Cette coordination sera essentielle pour faire en sorte que les rôles et les responsabilités soient aussi clairs, rationalisés et cohérents que possible, et pour éviter toute redondance, tout retard et toute confusion inutiles pour les particuliers qui souhaitent contester des décisions inexactes, injustes ou déraisonnables.

13. TENIR COMPTE DES CADRES D'ORIENTATION ET DE GOUVERNANCE EXISTANTS

Soulignons que nombre des défis relatifs à l'IA de confiance ne sont que de nouvelles variations de défis que le gouvernement a déjà relevés. Nous recommandons donc que le cadre fasse référence aux règlements, politiques, normes et lignes directrices existants et s'en inspire, le cas échéant, à la fois pour assurer une approche cohérente et pour permettre au gouvernement de mieux concentrer ses efforts sur les défis uniques de l'IA.

Par exemple, comme mentionné ci-dessus, le principe d'exactitude (et donc d'impartialité) figure déjà en bonne place parmi les obligations des institutions publiques assujetties à la LAIPVP. De même, bien que l'explicabilité soit particulièrement difficile à réaliser dans certains systèmes d'IA, la notion de « donner des motifs » est déjà une caractéristique de longue date du droit administratif. L'explicabilité peut également être soutenue par de solides pratiques de documentation et de tenue de dossiers, que les institutions gouvernementales doivent déjà appliquer. La transparence des processus gouvernementaux n'est pas non plus un concept nouveau. L'alignement sur les normes existantes, le cas échéant, pourrait contribuer à démystifier l'IA et à la normaliser en tant que composante des activités gouvernementales soumise à l'ensemble des mécanismes de gouvernance d'une institution.

14. CLARIFIER CE QU'EST UNE IA « AU SERVICE DE TOUS LES ONTARIENS ET ONTARIENNES »

Nous tenons aussi à vous faire part d'une dernière réflexion sur notre récent processus qui a conduit à la formulation de nos priorités stratégiques. Dans notre document de consultation initial, nous avons proposé une priorité éventuelle autour du thème suivant : « L'utilisation responsable des données pour le bien commun ». Au cours de

43 Gouvernement de l'Ontario. *Créer un Ontario numérique*, 30 avril 2021, **https://www.ontario.ca/fr/page/creer-un-ontario-numerique.**

l'élaboration de cette priorité, notre comité consultatif spécial[44] et d'autres intervenants nous ont fait clairement comprendre que le concept de « bien commun » n'était pas nécessairement très bien défini, et qu'il fallait se poser des questions : qu'est-ce que le bien commun? Le bien de qui, au juste? Qui prendra les décisions finales, et qui est responsable? Et enfin, quelles sont les limites à ne pas dépasser, même si les résultats visés sont souhaitables?

Ces questions semblent concorder avec l'engagement *Une IA qui est au service de tous les Ontariens et Ontariennes* et avec les mesures possibles qui y sont associées. La province devrait donc envisager une mesure possible qui permet de répondre d'emblée à ces questions essentielles. Au moment de « s'engager avec les dirigeants du secteur et de la société civile pour établir une norme encadrant "l'IA de confiance" et un processus permettant de valider que les fournisseurs respectent la norme gouvernementale », la province devrait mener des consultations plus larges sur ce que représente réellement une IA au service de tous les Ontariens et Ontariennes. Ce travail permettra de créer une base solide pour les mesures à venir, en clarifiant pour les concepteurs ce qu'ils doivent considérer comme étant des préjudices éventuels ou ce qu'une « norme d'IA de confiance » est censée accomplir.

CONCLUSION

En conclusion, nous félicitons le gouvernement d'avoir entrepris ce travail important et nous reconnaissons que la formulation de lignes directrices sur l'utilisation de l'IA par le gouvernement représente une première étape importante vers l'objectif global de bâtir une économie numérique alimentée par une IA de confiance.

Nous sommes impatients de collaborer avec la province à mesure qu'elle avance dans son travail sur le cadre proposé et les engagements connexes, et nous proposons de contribuer à ce travail dans le cadre de notre propre priorité stratégique de promouvoir la protection de la vie privée et la transparence dans un gouvernement moderne.

44 Commissaire à l'information et à la protection de la vie privée de l'Ontario. *Priorités stratégiques du CIPVP 2021-2025*, 22 avril 2021, annexe A, **https://www.ipc.on.ca/about-us/priorites-strategiques-du-cipvp-2021-2025/?lang=fr.**

Information and Privacy Commissioner of Ontario

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

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

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

Juin 2021