

Monsieur John Roberts  
Directeur général de la protection de la vie privée et archiviste de l'Ontario, et directeur général de la sécurité de l'information (A)  
Division de l'information, de la protection de la vie privée et des Archives publiques et Division de la cybersécurité  
Ministère des Services gouvernementaux et des Services aux consommateurs  
134 boul. Ian MacDonald  
Toronto, ON, M7A 2C5  
Envoyé par courriel : [John.Roberts@ontario.ca](mailto:John.Roberts@ontario.ca)

Cher John,

Voici la soumission de l'ABRC liée à la consultation du gouvernement de l'Ontario sur le cadre de l'intelligence artificielle (IA) de l'Ontario. La consultation a pris fin le 4 juin 2021. Ces informations ont également été soumises le 4 juin à l'aide du formulaire web prévu pour le processus de consultation.

**Veillez noter que** la présente lettre comprend les « commentaires supplémentaires » présentés par l'ABRC le 4 juin, mais nous avons également présenté un classement des mesures à prendre dans chaque catégorie du projet. En dépit de notre classement, nous estimons que chaque mesure est nécessaire dans le cadre de ce processus et que le gouvernement devrait les examiner à fond et les mettre en œuvre.

**1. À votre avis, quelles autres mesures doit-on inclure pour soutenir « Aucune d'IA en secret » dans le cadre de l'IA de l'Ontario ?**

L'objectif de cette section — veiller à ce que l'utilisation de l'IA par le gouvernement soit toujours transparente, juste et équitable — est louable ; ainsi, le gouvernement de l'Ontario et ses citoyens s'inquiètent à juste titre de l'association avec des entreprises d'IA et de l'utilisation par le gouvernement d'algorithmes pour des services ou des communications. Toutefois, comme vous le verrez dans nos commentaires, la nature évolutive de l'IA complique cet objectif.

De toute évidence, le processus doit être clair et transparent, et la transparence liée à l'IA doit être définie et utilisée dans l'intérêt public. Il doit y avoir des lois ou des règlements sur la durée de conservation des données des citoyens, sur la manière dont elles seront utilisées ou réutilisées ainsi que des restrictions sur la manière dont elles peuvent être partagées, revendues ou réorganisées sans l'autorisation explicite du sujet.

Les citoyens de l'Ontario ont le droit de consulter et de contrôler leurs données et de savoir comment leurs données seront utilisées et réutilisées par le gouvernement, sans accès par un tiers et sans avantage pour un tiers (comme la constitution d'un ensemble de données). En tant qu'entité fiable, le gouvernement de l'Ontario doit s'assurer qu'il fait un principe fondamental de l'utilisation éthique de la

technologie de l'IA et des algorithmes et du respect des données de ses citoyens. Les citoyens doivent avoir la certitude que leurs données ne seront utilisées qu'à des fins administratives et qu'ils ont la possibilité de refuser de partager leurs données et d'obtenir le service d'une autre manière. Les citoyens de l'Ontario ont le droit de posséder leurs données et de contrôler leur utilisation et leur réutilisation.

Le gouvernement doit confronter le fait que de nombreuses entreprises qui vendent des produits centrés sur l'IA sont intrinsèquement problématiques. Ces technologies peuvent renforcer les préjugés raciaux ([https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3333423](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423), <https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/>) et porter atteinte à la vie privée des citoyens. Bien qu'il existe de nombreux exemples problématiques de ce dernier type, les plus inquiétants sont les entreprises qui grattent des images sur Internet pour construire des bases de données massives d'informations biométriques sur les individus. Clearview AI, par exemple, a utilisé ce modèle pour son service de reconnaissance faciale, et son ensemble de données a été utilisé par de grandes entreprises et par les services de police pour identifier des individus. Heureusement, les activités de Clearview AI sont maintenant illégales au Canada (<https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html>). Or, il a fallu une enquête du New York Times (<https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>) et une étude du Commissariat à la protection de la vie privée du Canada ([https://priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c\\_210203](https://priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203)) pour en arriver là.

La communication d'informations biométriques — comme les photos de passeport ou de permis de conduire — à des entreprises externes comporte de nombreux risques. Par exemple, on ne sait pas toujours de quelle manière les données biométriques seront utilisées, malgré les professions de bonnes intentions des entreprises. Les gouvernements et les citoyens ont besoin de la protection de lois robustes pour protéger l'utilisation et la confidentialité des données, et de sanctions sévères et paralysantes en cas de violation de la loi. Il est inquiétant de constater que bon nombre de ces entreprises d'IA ont des liens avec l'extrême droite et les groupes de suprématie blanche (<https://medium.com/@AINowInstitute/ai-and-the-far-right-a-history-we-cant-ignore-f81375c3cc57>) et que ces points de vue peuvent se refléter dans les résultats de leurs algorithmes.

Contrairement aux fuites de données concernant les adresses électroniques et les mots de passe, qui sont facilement modifiables, les fuites de données incluant des informations biométriques, telles qu'une numérisation de l'iris, une empreinte digitale ou même une image du visage, qui sont liées à jamais à votre identité, peuvent causer des dommages incalculables. L'Ontario doit se distancer de telles entreprises et pratiques.

La COVID-19 a conduit à l'adoption massive de technologies de surveillance par les gouvernements du monde entier. Selon l'Electronic Frontier Foundation (EFF) :

Les gouvernements du monde entier réclament de nouveaux pouvoirs de surveillance exceptionnels (<https://www.eff.org/deeplinks/2020/12/covid-19-and-surveillance-tech-year-review-2020>) que beaucoup espèrent voir endiguer la propagation du virus. Cependant, beaucoup de ces pouvoirs empièteraient sur notre vie privée (<https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis>, entraveraient notre liberté d'expression (<https://www.eff.org/deeplinks/2020/04/some-covid-19-surveillance-proposals-could-harm-free-speech-after-covid-19>) et pèseraient de manière

disproportionnée sur les groupes de personnes vulnérables (<https://www.eff.org/issues/covid-19>).

Il faut à tout prix résister à ce type de « théâtre de la sécurité », car ces avantages minimes ou perçus se font souvent au détriment des droits à la vie privée (et autres) des citoyens. L'ensemble de la déclaration de l'EFF comprend un certain nombre de questions que les gouvernements doivent se poser lorsqu'ils envisagent ce type de technologies (<https://www.eff.org/issues/covid-19>).

Les outils d'éducation et de recherche permettant la surveillance universitaire et la marchandisation potentielle des données personnelles et professionnelles des individus dans les universités et les collèges devraient être soigneusement examinés et réglementés. Des exemples de problèmes causés par les technologies d'IA dans ce secteur sont décrits dans les articles suivants :

- Confronter les systèmes de surveillance alarmants mis en place par les fournisseurs des bibliothèques <https://sparcopen.org/news/2021/addressing-the-alarming-systems-of-surveillance-built-by-library-vendors/>
- Elsevier a déployé un outil de suivi des utilisateurs finaux pour des raisons de sécurité. Les utilisateurs doivent-ils s'inquiéter de leur vie privée ? <https://scholarlykitchen.sspnet.org/2020/10/13/elsevier-has-deployed-an-end-user-tracking-tool-for-security/>
- La vie privée des étudiants et la lutte pour maintenir l'espionnage hors des écoles : Bilan de l'année 2020 <https://www.eff.org/deeplinks/2020/12/student-privacy-and-fight-keep-spying-out-schools-year-review-2020>
- Les entreprises de détection de la tricherie ont gagné des millions pendant la pandémie. Au tour des étudiants à se défendre <https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/>. L'une des entreprises mentionnées dans cette histoire, Proctorio, est en litige avec un développeur pédagogique de l'Université de Colombie-Britannique pour avoir publié une série de gazouillis contenant des liens vers les vidéos de formation des professeurs de Proctorio, que l'entreprise considère comme confidentielles. Linkletter est un critique virulent des outils de « logiciel de surveillance universitaire », et cette action démontre la position agressive que cette industrie peut adopter pour faire taire ses critiques <https://www.insidehighered.com/quicktakes/2020/10/20/ed-tech-specialist-fights-proctorio-lawsuit>).

Pour ce qui est de la transparence, que signifie-t-elle dans ce contexte ? De quelle manière un citoyen peut-il savoir si un algorithme est transparent ? Existe-t-il une norme de transparence ? La transparence doit être définie d'une manière qui profite aux citoyens et qui offre à tous ceux qui interagissent avec les algorithmes d'IA la possibilité de faire examiner l'algorithme par des instances impartiales. Ce processus doit se dérouler rapidement et les résultats de cet examen devraient ensuite être accessibles au public. Les Ontariens doivent être informés lorsqu'ils interagissent avec des algorithmes d'intelligence artificielle ou des machines d'IA, avoir la possibilité de refuser une telle interaction et se voir présenter une autre façon d'interagir avec le gouvernement sans IA pour obtenir des renseignements ou des services. Un citoyen doit pouvoir demander une autre méthode de communication ; en aucun cas, un citoyen ne doit se voir refuser un service parce qu'il a choisi de ne pas utiliser les outils fondés sur l'IA.

Le gouvernement de l'Ontario et les Ontariens doivent faire face aux problèmes de l'IA en général, et avant tout déterminer des conditions d'utilisation appropriées qui respectent les droits des citoyens et empêchent les entreprises ou les gouvernements impliqués dans l'IA d'aller trop loin. L'acquisition des données des citoyens se produit déjà ; or, une réglementation à cet égard s'impose depuis longtemps. Nous devons examiner attentivement la manière dont le gouvernement de l'Ontario envisage d'aborder le manque flagrant de responsabilité des pratiques actuelles de collecte de données des citoyens par l'IA. Chaque contrat avec une tierce partie doit prévoir la suppression complète de toutes les données des citoyens après leur utilisation, y compris les données anonymes, car elles peuvent facilement être recombinaisonnées pour identifier une personne, sauf si chaque personne y consent.

**2. À votre avis, quelles autres mesures doit-on inclure pour soutenir « l'utilisation de l'IA en laquelle les Ontariens peuvent avoir confiance » dans le cadre de l'IA de l'Ontario ?**

Au minimum, des règles et des outils devraient être mis en place pour appliquer de manière sûre et sécurisée des algorithmes aux programmes et services gouvernementaux en fonction des risques. Cependant, cela est une fois de plus compliqué par la nature de l'IA et son opacité pour le citoyen moyen.

Comme notre réponse à la question 1 en témoigne, une approche basée sur le risque pour déterminer les règles applicables en matière de gouvernance de l'intelligence artificielle est une approche insatisfaisante pour protéger les droits des citoyens. Les droits des citoyens doivent passer en premier ; les réglementations gouvernementales doivent ainsi être mises en œuvre pour prévenir les abus de droit. Le modèle commercial actuel utilisé par de grandes entreprises technologiques comme Google et Amazon — agir en attendant d'être poursuivi en justice ou d'être traduit devant une commission gouvernementale — bafoue les droits des citoyens à la vie privée et à la protection des données. Les citoyens se trouvent dans un scénario de type « David et Goliath » où le citoyen moyen peut être alarmé, mais ne sait pas comment protéger ses droits. Une gouvernance adéquate des algorithmes d'intelligence artificielle et une réglementation de l'utilisation de l'IA par les grands intermédiaires en ligne et les établissements d'enseignement financés par les fonds publics sont essentielles à la protection des droits des citoyens de l'Ontario. L'idée que les entreprises privées ou les gouvernements provinciaux ou fédéraux puissent s'autogouverner sans lois et règlements et sans surveillance appropriée est contraire aux principes de bonne gouvernance que sont la responsabilité, l'intégrité, l'intendance et la transparence.

Au fond, les gouvernements doivent respecter les principes d'éthique, d'équité, de justification, de transparence et d'options de retrait pour l'utilisation des algorithmes d'IA à des fins gouvernementales et pour la prise de décision.

Notre réponse à la question 1 illustre également l'impact négatif des systèmes de décision automatisés (SDA). Les systèmes de décision automatisés, utilisés dans le processus décisionnel du gouvernement, souffrent de la « personne derrière la machine » — soit celui qui a créé le système et les préjugés y sont intégrés par conséquent. L'exclusion des préjugés est extrêmement difficile et il a été démontré que les SDA ont des effets néfastes sur les groupes méritant l'équité ou privés d'équité. Les entreprises technologiques externes n'ont peut-être pas l'expertise nécessaire pour effectuer un examen approfondi de la partialité que les gouvernements et les organisations d'intérêt public exigeraient ; on

ne devrait donc pas leur faire confiance pour le faire. La manière dont cet examen est effectué ou le nombre d'examineurs utilisés auront des conséquences importantes sur le véritable dépistage des biais. Des processus doivent absolument être mis en place pour garantir que les algorithmes sont continuellement testés et évalués quant aux risques et à la partialité.

Selon l'Institut AI Now, « Lorsque l'intelligence artificielle et les technologies connexes sont utilisées pour prendre des décisions et faire des prédictions dans des domaines dont les enjeux sont importants, tels que la justice pénale, l'application de la loi, le logement, l'emploi, l'embauche et l'éducation, elles peuvent avoir une incidence profonde sur les droits et libertés fondamentaux. »

(<https://ainowinstitute.org/>)

### **3. À votre avis, quelles autres mesures doit-on inclure pour soutenir « l'IA au service de tous les Ontariens » dans le cadre de l'IA de l'Ontario ?**

Le gouvernement de l'Ontario est parfaitement conscient des cadres utilisés par le gouvernement fédéral et par d'autres régions qui aideront à atteindre cet objectif. Le gouvernement fédéral a une [Directive sur la prise de décisions automatisée](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592&section=html) : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592&section=html> qui rend obligatoire la pratique des évaluations d'impact algorithmique et tente d'intégrer plus de transparence dans le processus pour les Canadiens. Pourtant, il y a bon nombre de ressources et d'outils pouvant aider le gouvernement de l'Ontario à concevoir un cadre au service de tous les Ontariens pour n'utiliser que des « technologies d'IA centrées sur les droits individuels et reflétant les diverses communautés de la province. »

Le gouvernement de l'Ontario doit, au minimum :

- Lire tous les rapports créés par l'Institut AI Now de l'Université de New York. Ce dernier est d'un centre de recherche interdisciplinaire consacré à la compréhension des implications sociales de l'intelligence artificielle. Voici une liste de leurs publications : <https://ainowinstitute.org/reports.html> ;
- Examiner attentivement les points soulevés par l'EFF dans son article intitulé *Covid-19 and Digital Rights* à l'adresse suivante : <https://www.eff.org/issues/covid-19>, et sa page sur l'IA en générale : <https://www.eff.org/issues/ai> ;
- Examiner les critiques des systèmes mis en place dans d'autres régions. Par exemple, AlgorithmWatch présente ici une critique complète des lacunes de l'IA fiable : <https://algorithmwatch.org/en/trustworthy-ai-is-not-an-appropriate-framework/>. Bien qu'elles soient écrites d'un point de vue européen, de nombreuses publications d'AlgorithmWatch peuvent aider à informer les actions en Ontario : <https://algorithmwatch.org/en/publications/>.

Lors de la conception de ce processus, le gouvernement de l'Ontario doit prêter une attention particulière aux exigences des communautés autochtones ayant droit à la pleine souveraineté sur leurs données en vertu de la Déclaration des Nations Unies sur les droits des peuples autochtones (DNUDPA). La souveraineté des données supposerait que les gouvernements et les chercheurs permettent à ces peuples et à leurs communautés de conserver la propriété et le contrôle de leurs propres données, et que toute utilisation de ces données soit totalement transparente et ne soit effectuée qu'après une consultation exhaustive.

Pour plus d'informations, consultez les ressources suivantes :

- Les principes de PCAP® des Premières Nations | Le Centre de gouvernance de l'information des Premières Nations <https://fnigc.ca/ocap-training/>
- La souveraineté des données autochtones : [https://fnigc.ca/wp-content/uploads/2020/09/bbe195ddc231e3b1222d71ca4c09ae62\\_indigenous\\_data\\_sovereignty\\_toward\\_an\\_agenda\\_11\\_2016.pdf](https://fnigc.ca/wp-content/uploads/2020/09/bbe195ddc231e3b1222d71ca4c09ae62_indigenous_data_sovereignty_toward_an_agenda_11_2016.pdf)
- La Déclaration des Nations Unies sur les droits des peuples autochtones <https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html>

Jusqu'à ce que le public comprenne la propriété et les droits sur ses données et les menaces substantielles que représentent les interfaces centrées sur l'IA, il faudrait envisager un moratoire ou une utilisation extrêmement limitée par le gouvernement des algorithmes d'IA et des outils connexes. Le gouvernement de l'Ontario doit commencer par adopter une loi conférant la propriété des données à chaque citoyen et empêcher les contrats de priver les citoyens de leur droit à la vie privée.

La possibilité pour les citoyens d'exprimer librement leurs idées et leurs points de vue est essentielle à une société libre et démocratique. Ils devraient également avoir l'option de se retirer des algorithmes et des opérations de l'IA s'ils le veulent. La liberté d'expression est un droit fondamental et un principe de base des bibliothèques, archives et musées (BAM). La surveillance et la crainte d'un contrôle des idées et des opinions portent fondamentalement atteinte aux droits les plus fondamentaux de la personne. La possibilité de suivre l'activité en ligne des individus par le biais de l'IA porte atteinte au droit à la vie privée et empiète sur d'autres droits de la personne, notamment la liberté intellectuelle ; la réglementation accrue d'Internet menace aussi le principe de neutralité du réseau, portant ainsi atteinte aux droits de la personne, notamment le droit d'accès à l'information.

Dans l'état actuel des choses, l'IA pose un risque important pour les droits de tous les Ontariens et nous félicitons le gouvernement d'avoir pris des mesures pour comprendre et atténuer les risques encourus.

Nous vous remercions de nous donner l'occasion de répondre à cette consultation. Si vous avez d'autres questions ou si vous souhaitez que nous assurions le suivi de certains points d'intérêt, n'hésitez pas à nous contacter.

Susan Haigh  
Directrice générale