CONSULTATION POPULAIRE SUR L'INTELLIGENCE ARTIFICIELLE

CONTRIBUTION PRÉSENTÉE PAR

MARS 2026

Table des matières

Présentation de la Ligue des droits et libertés

La Ligue des droits et libertés (LDL) est une organisation indépendante, non partisane et sans but lucratif, qui vise à défendre et à promouvoir les droits humains en mettant de l'avant leur universalité, leur indivisibilité et leur interdépendance. Depuis sa création en 1963, la LDL a influencé plusieurs politiques gouvernementales et projets de loi en plus de contribuer à la création d'instruments et d'institutions voués à la défense et la promotion des droits humains, tels que la *Charte des droits et libertés de la personne* du Québec et la Commission des droits de la personne et des droits de la jeunesse (CDPDJ).

Elle intervient régulièrement dans l'espace public pour porter des revendications et dénoncer des violations de droits humains auprès des instances gouvernementales sur la scène locale, nationale ou internationale. La LDL est également membre de la Fédération internationale pour les droits humains (FIDH). La LDL poursuit, comme elle l'a fait tout au long de son histoire, différentes luttes contre la discrimination et contre toute forme d'abus de pouvoir, pour la défense des droits civils, politiques, économiques, sociaux et culturels qui sont universels, interdépendants et indissociables.

Introduction

En réponse aux développements vertigineux des technologies d'intelligence artificielle (IA) et à la suite de consultations-éclairs qui ont fait l'économie d'un véritable débat public, Evan Solomon, ministre de l'IA et de l'Innovation numérique, a exprimé sa volonté de mettre rapidement en œuvre une politique axée sur « l'IA pour tous ». Cette IA, a-t-il assuré, reposera sur la « confiance, la sécurité et la responsabilité ». Le ministre ambitionne de plus de voir le Canada devenir un « puissant centre d'IA ».

On ne peut nier certains avantages indéniables de ces technologies, par exemple dans le domaine de la santé et de la recherche scientifique (outils de diagnostic alimentés par l'IA qui font preuve d'une précision remarquable; capacité d'analyse de quantités gigantesques de données). Ainsi, depuis quelque temps, le battage médiatique est incessant sur le besoin d'investir et d'adopter ces technologies afin de demeurer « compétitifs » et de stimuler l'économie et l'innovation.

Néanmoins, des questions demeurent quant à ce qui motive vraiment l'innovation et le déploiement accéléré de l'IA : outre les promesses du bien commun, l'IA est appelée à procurer à ses plus importants détenteurs, grâce notamment à la mainmise sur les données tant publiques que privées, un immense pouvoir. **L'IA accélère également la mainmise du privé sur le secteur public.** De plus, l'introduction de l'IA et sa capacité de traitement sans précédent risquent aussi par la même occasion d'instaurer une surveillance en continu et à grande échelle à l'insu des citoyen·nes.

Ainsi, la société civile soucieuse de préserver les droits et libertés hésite; d'un côté, il y a l'espoir d'un progrès prodigieux dans plusieurs domaines et, de l'autre, la menace éventuelle d'être dépassée par des technologies toujours plus puissantes. Certains évoquent même le risque d'une mise à l'écart des humains dans de nombreux secteurs de l'emploi.

En l'absence d'encadrement et de réglementations de l'IA, les voix qui expriment de graves préoccupations ne se comptent plus[1]. Ces voix nous signalent que les technologies révolutionnaires de l'IA, malgré leurs avantages, ouvrent aussi la voie à des bouleversements perturbateurs de nos sociétés : militarisation de l'IA; potentiel de pertes d'emploi massives dans le secteur privé et public (notamment si l'IA agentique[2] entre en jeu); montée de la pauvreté et des inégalités; voracité énergétique et hydrique des centres de données[3], appropriation des données et du savoir autochtone; contrôle et surveillance massive des populations; affaiblissement des institutions démocratiques et de la protection de la vie privée. Enfin, jamais dans l'histoire les États, la Big Tech et le Big Data n'auront disposé d'instruments de surveillance et de contrôle aussi puissants et sophistiqués.

Ainsi, inquiète du potentiel néfaste de certaines technologies d'IA sur la protection des droits et des libertés, la Ligue des droits et libertés (LDL) appelle à la mise en place de législations et réglementations aptes à encadrer leur usage et leur développement dans la transparence, afin qu'elles demeurent au service du bien commun.

Nous soulignons plus bas certaines de nos principales préoccupations, en suivant la structure proposée par le Guide de consultation avancée.

2. Utilisations actuelles et potentielles de l'IA

Dans cette section, nous présentons des préoccupations liées au double usage vers lesquelles s'orientent les technologies de l'IA. L'entreprise Palantir, très présente aux États-Unis et au Royaume-Uni dans les secteurs civil comme militaire, constitue l'exemple le plus marquant de plateformes numériques dont les modèles posent un défi à la gouvernance démocratique et aux libertés civiles.

La frontière entre applications civiles et militaires de l'IA s'estompe.

Plus qu'un logiciel neutre, l'IA avancée est un outil intrinsèquement voué au double usage, puisque ses « innovations » intéressent autant les secteurs civils que militaire. Dans un article de La Presse intitulé « *L'IA s'en va-t-elle en guerre*?[4] », Karim Jerbi, directeur du Centre de recherche québécois en neurosciences et en intelligence artificielle, affirme que « l'intégration des grands modèles d'IA au complexe militaro-industriel » est profondément inquiétante. De plus, aucun cadre juridique international n'a encore été établi pour en encadrer l'usage. Le récent différend éthique qui a opposé Anthropic et le Pentagone quant à la pertinence d'imposer certaines lignes rouges dans l'usage du logiciel Claude pour la surveillance de masse intérieure et pour l'usage d'armes entièrement autonomes a de quoi, insiste l'article, inquiéter toute la planète.

Le débat actuel autour des technologies avancées d'IA se situe en outre dans une époque marquée par une indifférence croissante, sinon une mise à l'écart totale et décomplexée par certains États de

[1] https://pauseai.info/quotes
[2] https://agenticstate.org
[3] Des mouvements contre ces centres semblent se multiplier : https://time.com/7377579/ai-data-centers-people-movement-cover
[4] https://www.lapresse.ca/affaires/techno/2026-03-04/vie-numerique/l-ia-s-en-va-t-en-guerre.php

la Charte des Nations Unies, du droit international des droits humains (DIDH) et du droit international humanitaire (DIH). On peut observer les effets catastrophiques pour les civils du déploiement des grands modèles d'IA (notamment les "chaînes de destruction", ou "kill chain" assistée par IA) lors d'opérations militaires et de surveillance, sans considération du DIH, dans les théâtres de guerre en Ukraine, à Gaza et en Iran.[5] Or, le DIH impose des obligations aux États et aux acteurs non étatiques quant à la conduite des hostilités, notamment les principes de distinction, de proportionnalité et de précaution. La question se pose donc de savoir si les entreprises technologiques qui fournissent en connaissance de cause des systèmes d'IA intégrés dans des chaînes de destruction pourraient engager leur responsabilité pour complicité dans des violations graves du droit international, tels que crimes contre l'humanité et crimes de guerre.

Dirigée par des entrepreneurs[6] hostiles aux principes démocratiques et réfractaires à toute réglementation, Palantir a construit pour un large éventail de clients une architecture numérique qui rend possible « une surveillance généralisée, une prise de décision préventive, une militarisation imperceptible de chaque institution »[7]. De plus, en 2025, le président Trump a chargé cette société de créer une infrastructure de données centralisée sur la population américaine[8].

L'objectif de l'entreprise, comme l'a déclaré l'un de ses dirigeants en 2021[9], est de devenir « le système d'exploitation du gouvernement américain ». Cette ambition se déploie aussi au Royaume-Uni, où elle met sa technologie de pointe à profit dans tous les secteurs de l'appareil d'État[10], au grand dam de la société civile. Enfin, il y aurait lieu de se demander à quel point la concentration de données, et donc de pouvoir, dans les mains de Big Tech investies dans les secteurs civil et militaire, minera la démocratie[11] et les libertés civiles[12].

Au Canada, une vigilance accrue de la part de la société civile s'impose quant aux usages potentiels de l'IA dans les infrastructures étatiques et dans la gouvernance.

Au Canada, une certaine militarisation de l'économie s'est amorcée avec la Loi du budget C-15, qui prévoit une augmentation significative des dépenses militaires afin de « rencontrer les défis d'un contexte géopolitique en évolution ». Cela inclut des investissements en IA et en informatique quantique qui visent à rendre l'IA plus puissante, ainsi que la création de BOREALIS. Ce nouveau centre de recherche se concentre sur les technologies émergentes à double usage, lesquelles sont considérées vitales pour les intérêts nationaux du Canada en matière de défense et de sécurité[13].

---

[5] https://bylinetimes.com/2026/03/05/palantirs-double-conflict-of-interest-in-the-war-against-iran
[6] https://asiatimes.com/2025/05/the-most-dangerous-man-in-america-isnt-trump-its-alex-karp
[7] https://www.authoritarian-stack.info/
[8] https://thenewamerican.com/us/tech/palantir-to-build-centralized-database-on-americans/
[9] https://www.frenchweb.fr/palantir-lentreprise-qui-reve-de-devenir-loperating-system-de-letat-americain/453670
[10] https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley
[11] https://www.nytimes.com/2026/03/17/opinion/ai-economy-trump-future.html
[12] https://www.authoritarian-stack.info ; https://www.monde-diplomatique.fr/2025/11/BRIA/68925
[13] https://www.canada.ca/fr/ministere-defense-nationale/programmes/borealis.html

Par ailleurs, la société civile s'inquiète de découvrir enfouie dans la Loi du Budget une clause « Henri VIII »[14] qui permettrait à certaines entités ou personnes de se voir accorder une exemption de toute loi fédérale (sauf criminelle) pour une période de trois ans, renouvelable, dans le but d'encourager notamment « l'innovation ». Selon ses critiques, cette clause, qui vise en particulier le secteur technologique, « dynamite » au passage la règle de droit[15]. Une telle clause permettrait-elle aux technologies d'IA d'échapper aux lois du travail, de la protection de l'environnement, de la santé publique, de la protection de la vie privée?

D'autre part, le budget introduit le concept de double usage. Celui-ci sous-tendrait l'ensemble des dépenses, incluant les investissements dans l'IA, l'informatique quantique et les biotechnologies, lesquels vont inévitablement déboucher sur des applications à la fois militaires et commerciales[16]. L'introduction de ce concept signale, selon deux chercheurs, la militarisation tranquille[17] de l'écosystème canadien de l'IA, lequel s'est longtemps distingué par son caractère « éthique ». Ce changement s'opère aussi dans le contexte d'un vide réglementaire.

En ce qui a trait à des utilisations potentielles préoccupantes de l'IA, le Canada a annoncé ces derniers mois des accords de coopérations sur l'IA avec Israël et le Royaume-Uni. Or, l'engagement avec Israël en matière d'IA[18] a été annoncé alors que ce pays accumule les accusations de génocide en Palestine, crime facilité par les technologies d'IA selon un rapport onusien[1920]. Israël est déjà connu comme un laboratoire[21] pour les technologies de contrôle social, de surveillance de masse, et de violence létale automatisées sur les populations civiles (amplifiées par les Palantir, Microsoft, Oracle, et autres), sans compter l'instrumentalisation à des fins néfastes d'appareils d'usage civil[22] (par ex. les téléavertisseurs au Liban[23]). Que le Canada salue des « échanges réguliers » avec Israël en matière de technologies et d'IA devrait-il nous alarmer?[24] On est en droit d'exiger que le Canada s'assure que sa coopération en matière d'IA ne contribue pas à des crimes de guerre ou à des crimes contre l'humanité.

---

[14] La "clause Henri VIII" de la Loi du Budget C-15, section 5 de la Partie 5, « autorise tous les ministres à exempter toute personne physique ou morale de l'application de toute loi fédérale canadienne dont ils sont responsables (à l'exception du Code criminel). Ces exemptions doivent simplement être justifiées comme étant « dans l'intérêt public » et « encourageant l'innovation, la compétitivité ou la croissance économique ».

[15] https://nationalpost.com/news/committee-amends-liberal-clause-in-budget-bill-that-critics-say-dynamites-the-rule-of-law ; https://ecojustice.ca/news/open-letter-to-federal-parliamentarians-to-remove-henry-the-viii-exemption-powers-from-budget-bill-c-15/

[16] https://www.linkedin.com/pulse/canadas-age-dual-use-spending-defence-sovereignty-da-mota-ph-d--1rifc

[17] https://www.ledevoir.com/opinion/idees/955905/militarisation-tranquille-ia-canadienne

[18] https://fr-cjpme.nationbuilder.com/no_israeli_ai

[19] https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf

[20] L'armée israélienne a développé des systèmes d'intelligence artificielle, tels que « Lavender », « Gospel » et « Where's Daddy ? », pour traiter des données et générer des listes de cibles,105 remodelant la guerre moderne et illustrant la nature à double usage de l'intelligence artificielle.

[21] https://www.versobooks.com/en-ca/products/2684-the-palestine-laboratory

[22] https://the307.substack.com/p/former-mossad-chief-brags-that-israel ; https://the307.substack.com/p/revealed-israel-used-palantir-technologies

[23] https://www.ohchr.org/en/press-releases/2024/09/exploding-pagers-and-radios-terrifying-violation-international-law-say-un

[24] https://www.middleeastmonitor.com/20251030-ex-mossad-chief-behind-icj-blackmail-campaign-brags-israel-has-installed-a-global-sabotage-network/

Pour ce qui est de la coopération avec le Royaume-Uni, le Canada a signé un protocole d'entente[25] sur la coopération dans le domaine du gouvernement numérique et de l'économie numérique. Il « permettra aux systèmes nationaux de se connecter et de jeter les bases de la création d'un réseau de nouvelle génération véritablement mondial, et de soutenir l'innovation au chapitre de l'infrastructure numérique essentielle ».

Or, selon un article du magazine The Nerve, Palantir se fait omniprésente dans les structures de l'État britannique[26], résultat d'un processus progressif, mais peu transparent[27], d'accumulation de contrats. Ceux-ci couvrent autant la gestion des données des patients du Service national de la Santé – Amnistie internationale appelle à un désengagement total de ces contrats[28] – que les opérations de défense, les bases de données de renseignements de la police, et la gestion des armes nucléaires.

En juillet 2025, le Canada a annoncé, dans une perspective « souverainiste », un partenariat avec Cohere, entreprise canadienne spécialisée dans le développement de grands modèles de langage, lui allouant 240 millions de dollars pour la mise sur pied de l'écosystème canadien d'IA et de services internes d'IA. Cependant, peu de détails sont disponibles, déplore l'Institut professionnel de la Fonction publique du Canada,[29] qui note que si Cohere arbore un drapeau canadien, cette société tire 90% de son chiffre d'affaires à l'étranger et fait appel à la société américaine CoreWeave pour gérer ses centres de données. Enfin, le site AInvest saluait en 2024 l'avènement d'un « puissant partenariat entre des entreprises de premier plan que sont Cohere et Palantir » qui « joueront un rôle crucial dans la construction de l'avenir de l'IA »[30].

Au Canada, outre deux contrats passés avec la Défense nationale (Palantir Gotham et Palantir Foundry), la présence directe de Palantir demeurerait modeste[31]. Toutefois, compte tenu d'une coopération croissante du Canada avec l'étranger, il y a lieu de se demander si ce type de technologies ouvrant la voie à la surveillance ne risque pas de s'introduire au pays de façon indirecte.

- Compte tenu des risques potentiellement néfastes de l'IA pour la démocratie et la protection des données, la mise en place d'un registre public de l'IA paraît essentielle en ce qui concerne les entreprises qui fournissent aux gouvernements l'infrastructure en IA. Il est également incontournable pour maintenir la confiance du public dans les technologies d'IA avancées;

---

[25] https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2025/12/le-canada-et-le-royaume-uni-renforcent-leurs-liens-dans-le-domaine-de-linfrastructure-quantique-et-numerique.html

[26] https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley

[27] https://www.theguardian.com/politics/2026/feb/05/calls-to-halt-uk-palantir-contracts-grow-amid-lack-of-transparency-over-deals

[28] https://www.amnesty.org/en/latest/news/2026/03/uk-global-human-rights-and-health-groups-in-new-briefing-urge-hospitals-not-to-use-palantir-software-and-demand-that-nhs-england-cancels-the-contract-entirely/

[29] https://pipsc.ca/fr/

[30] https://www.ainvest.com/news/cohere-and-palantir-a-powerful-ai-partnership-24121010a7c24aeeefc720fa/

[31] Voir la réponse à la question Q-8 [Palantir] by Cheryl Gallant (Algonquin—Renfrew—Pembroke), May 27, 2025 = Q-8 [Palantir] de Cheryl Gallant (Algonquin—Renfrew—Pembroke), le 27 mai 2025, Bibliothèque du Parlement. https://parl-gc.primo.exlibrisgroup.com/discovery/delivery/01CALP_INST:01CALP/12177592250002616?lang=en

- De façon plus générale, l'innovation ne doit pas être exemptée de critères et garde-fous éthiques et de sécurité, ni du respect des lois fédérales (clause Henri VIII de la Loi du Budget);
- Des entreprises d'IA dont les valeurs vont à l'encontre des principes démocratiques et des droits humains devraient être exclus du secteur public;
- Le Canada, en sa qualité de leader dans le domaine de l'IA, pourrait s'appuyer sur la Déclaration de Montréal pour un développement responsable de l'IA et s'opposer à sa militarisation;
- Le Canada devrait s'assurer que ses engagements de coopération, ses contrats et son financement dans le secteur de l'IA respectent ses obligations en vertu du droit international, et exclure tout acteur dont les technologies contribuent à des crimes de guerre ou à des crimes contre l'humanité.

3. Main-d'œuvre

(b) Quel est l'impact de l'IA sur les droits du travail ou d'autres questions liées au travail ?

(c) Comment certains types de travail (par exemple, les emplois précaires, les entrepreneurs indépendants) ou certains secteurs d'activité (par exemple, l'industrie manufacturière, l'agriculture, les soins de santé, les arts créatifs) sont-ils particulièrement touchés par l'IA ?

(d) Quel est l'impact de l'IA sur les relations entre employeurs et employés ?

L'introduction de l'intelligence artificielle en emploi soulève de nombreuses préoccupations.

Suppression ou modification d'emplois

Selon une étude de l'Organisation Internationale du Travail, les pertes d'emploi dues à l'IA générative seront relativement faibles, mais les effets seront substantiels pour les employé·es de bureau, majoritairement des femmes (service à la clientèle, réceptionnistes, secrétaires, etc.). Celles-ci sont deux fois et demi plus exposées aux risques d'automatisation que les hommes[32].

L'Institut du Québec évalue de son côté qu'environ 810 000 personnes, soit 18% de la main-d'œuvre québécoise, travaillent ou cherchent un emploi dans 96 professions actuellement vulnérables à l'automatisation. Les groupes les plus à risque sont les femmes, la population immigrante et les minorités visibles, la main-d'œuvre expérimentée (plus âgée) et les jeunes[33].

Bien d'autres secteurs que les emplois de bureaux pourraient être touchés. Selon une analyse de Anthropic les emplois de professionnels suivants sont vulnérables : programmeurs ; conseillers clientèle, opérateurs de saisie, spécialistes des dossiers médicaux, analystes d'études de marché ou

[32] https://www.ilo.org/fr/resource/article/minimiser-les-effets-negatifs-du-chomage-technologique-induit-par-lia

[33] https://institutduquebec.ca/publications/repercussions-de-l-automatisation-et-de-l-ia-sur-la-main-d-oeuvre-au-quebec

spécialistes marketing[34]. Sans compter les emplois en culture (production de films, d'images, de textes, de voix, etc.)

L'IA pourrait aussi entraîner la transformation importante de certains emplois ou la création de nouveaux postes, nécessitant une requalification des salarié·es. Cela pourrait s'avérer difficile pour les travailleur·euses plus âgé·es ou moins scolarisé·es.

Il va sans dire, par ailleurs, que les avancées fulgurantes en matière d'IA, notamment l'IA agentique (capable d'analyser des données, de planifier des étapes et de prendre des décisions autonomes pour atteindre un objectif fixé), pourraient mener, dans le futur, à la suppression ou à la transformation de bien d'autres types d'emplois.

Le dialogue social et des politiques de soutien au revenu, de requalification et de transitions numériques seront essentiels pour soutenir les travailleurs et travailleuses concerné·es.

Santé-sécurité

Intensification du travail

L'adoption de l'IA en vue d'optimiser les tâches et d'accroître la productivité peut entraîner une intensification inacceptable du travail. Comme le souligne l'Agence européenne pour la sécurité et la santé au travail (EU-OSHA) :

> L'IA engendre cela, notamment en émettant des recommandations et instructions en temps réel destinées aux travailleurs sur la manière d'effectuer leur travail, ce qui peut également les pousser à travailler plus vite et induire davantage de stress professionnel, d'effets néfastes sur leur santé physique et d'accidents.[35]

L'accroissement du rythme de travail et l'obligation de suivre les instructions de l'IA en temps réel (ex. Amazon) entraîne du stress et peut générer des accidents de travail.

Taylorisation numérique

L'IA peut entraîner une perte d'autonomie et de contrôle des salarié·es sur leur travail. C'est l'humain qui, peu à peu, est mis au service de la machine :

> L'IA remet au goût du jour un taylorisme, cette fois-ci numérique, qui réduit chaque employé à un maillon silencieux et passif de la grande chaîne de production. Le travail, autrefois source de fierté et de sens, semble peu à peu perdre son âme[36].

---

[34] https://www.futura-sciences.com/tech/actualites/intelligence-artificielle-anthropic-mis-point-detecteur-reperer-metiers-ia-pourrait-faire-disparaitre-132630/

[35] https://healthy-workplaces.osha.europa.eu/en/publications/summary-artificial-intelligence-worker-management-overview

[36] https://www.revuegestion.ca/lintelligence-artificielle-nuirait-elle-au-bien-etre-des-employes

Surveillance et atteinte à la vie privée

Une autre forme de déshumanisation du travail survient lorsque la personne salariée est considérée comme une donnée parmi d'autres, un élément de production à surveiller et à évaluer :

> Cette déshumanisation peut être qualifiée de « mise en donnée » du lieu de travail, sur lequel les travailleurs ne sont plus traités comme des êtres humains, mais comme des recueils de données numériques objectives qu'ils ont produites dans le cadre de leur travail.[37]

La surveillance des personnes salariées, souvent cachée ou ignorée, et l'évaluation algorithmique de leur travail compromettent le droit à la vie privée et à la dignité.

Relation de travail et syndicalisation

Les transformations qu'entraîne l'IA dans le monde du travail vont bien au-delà de la négociation de convention collective. Il est essentiel d'assurer la participation des personnes salariées et de leurs syndicats aux discussions sur les changements de politiques socio-économiques et législatives nécessaires pour une utilisation éthique des nouvelles technologies.

Par ailleurs, le droit à la syndicalisation demeure essentiel. Dans certains secteurs, l'IA offre de nouvelles possibilités de remplacement des employé·es. Et la capacité de s'organiser collectivement pour faire face à l'employeur est alors déterminante. On l'a vu récemment dans l'industrie du cinéma (scénaristes, acteurs et doubleurs de cinéma, de télévision et de jeux vidéo) où une grève historique a permis de limiter un peu l'utilisation abusive de l'IA[38].

Mais dans plusieurs secteurs d'emploi, la syndicalisation demeure quasi impossible. Ainsi, les travailleurs et travailleuses de plateforme numérique (livraison, transport, micro-tâches, création de contenu) sont dans une situation d'isolement et de vulnérabilité qui les privent de tout pouvoir de négociation. Faussement qualifiés de travailleurs indépendants, ils se trouvent exclus du « statut de salarié » qui leur permettrait de bénéficier des protections que confèrent les lois du travail. **Des modifications législatives s'imposent pour que ces formes atypiques d'emploi (notamment relation tripartite d'emploi) bénéficient des mêmes protections légales (syndicalisation, protection sociale, santé-sécurité) que ceux qu'octroie la relation classique d'emploi.**

---

[37] https://healthy-workplaces.osha.europa.eu/en/publications/summary-artificial-intelligence-worker-management-overview

[38] https://intelligence-artificielle.developpez.com/actu/350511/Les-greves-a-Hollywood-sont-desormais-terminees-les-acteurs-ont-conclu-un-accord-avec-les-studios-prevoyant-des-protections-contre-l-utilisation-non-autorisee-d-images-generees-par-IA/

4. Impacts environnementaux et centres de données

(a) Quels sont les enjeux et les implications de l'IA pour l'environnement et les changements climatiques ?

La croissance illimitée de l'économie fondée sur les données (capitalisme de surveillance ou capitalisme algorithmique) est incompatible avec la lutte contre les changements climatiques et les efforts pour protéger l'environnement. Selon l'Agence internationale de l'énergie (AIE), l'IA sera la première responsable de la croissance des centres de données et représentera la moitié de la croissance de demande d'électricité aux États-Unis d'ici 2030. Toujours selon l'AIE, la consommation des centres de données dans le monde va plus que doubler d'ici 2030 pour équivaloir à celle du Japon, pays de 125 millions d'habitants. De plus, pour des raisons pratiques (approvisionnement fiable 24 heures sur 24) les centres de données ont souvent recours à des sources d'énergie polluantes.

Mais même les énergies « vertes » ne règleront pas le problème. Les énergies dites « vertes » ont également une empreinte carbone et un impact climatique et environnemental. **La réduction de l'empreinte carbone de la production d'énergie requiert non seulement un transfert de production vers des énergies « vertes », mais surtout une réduction de la demande énergétique incompatible avec un développement tous azimuts de l'IA.**

L'impact environnemental de l'IA ne se limite pas à la production d'énergie. Le fonctionnement des centres de données nécessite des quantités importantes d'eau, alors que les conflits d'usage de cette ressource ne cessent de croître. L'eau accaparée par les centres de données se fait au détriment du droit à l'eau comme droit humain et à des usages essentiels, comme l'agriculture.

Le Rapporteur spécial sur les droits à l'eau et à l'assainissement appelait en 2025 à un moratoire sur la construction de centre de données, déplorant que le manque de transparence de ce secteur et son impact considérable sur la consommation d'énergie et d'eau constituent des menaces mondiales[39].

(b) Quel est l'impact d'une mise à fond sur l'IA sur l'approche du Canada en matière de ressources naturelles, d'énergie, d'émissions de carbone et d'autres formes de pollution (air, eau, sol), tant au niveau des politiques locales que dans la vie quotidienne des individus ?

L'orientation du gouvernement du Canada, qui fait de l'IA un axe de développement stratégique, ne peut être dissociée de sa volonté de faire du Canada un producteur de minéraux critiques et de sa politique de militarisation. Les matériaux essentiels au développement de l'IA et des centres de données (terres rares, lithium, graphite...) sont les mêmes que ceux de l'industrie militaire. Ces projets miniers ont partout un impact environnemental catastrophique. Une mine propre, ça n'existe pas et les mines pour les matériaux comme les terres rares sont particulièrement destructrices. Le matériau recherché est présent en très petite proportion dans le minerai extrait, ce qui engendre d'immenses mines (en général à ciel ouvert) et surtout des quantités phénoménales de déchets toxiques issus du traitement du minerai. En plus de polluer le territoire, ces installations consomment une immense quantité d'eau. **Ces activités portent atteinte au droit à l'eau et à un environnement sain des**

[39] https://blue-community.net/2025/10/un-moratorium-on-data-center-construction/

populations du territoire, qui sont très souvent autochtones. Dans le cas des Autochtones, cela pose également la question de la consultation et du consentement qui ne sont généralement pas respectés.

> *(c) Quels sont vos enjeux et vos préoccupations concernant la construction de centres de données d'IA ?*
>
> *(d) Y a-t-il des enjeux ou des implications différents selon l'emplacement où un centre de données est construit (par exemple, dans une communauté rurale, sur une île, sur des territoires autochtones) ? Si oui, quels sont-ils ?*

La surface occupée par les centres de données ne peut plus être ignorée. La dimension d'un centre peut équivaloir à plusieurs terrains de football et il y en a des milliers dans le monde. Quel que soit l'emplacement, les centres de données accaparent du territoire qui pourrait être utilisé à d'autres fins. Les centres auront évidemment un impact d'autant plus négatif s'ils accaparent des terres agricoles ou impliquent la destruction de milieux de grande valeur écologique, comme les milieux humides.

> *(e) Quelles sont les préoccupations et les avantages liés au développement de centres de données au Canada ?*

Le développement des centres de données et de l'IA devrait être limité à des usages socialement utiles. Ces usages devraient faire l'objet d'un débat public. **Par ailleurs, dans l'intérêt de protéger les données de la population, des centres de données sur le territoire, et sous contrôle des gouvernements, sont absolument essentiels.**

> *(f) Quels dangers ou avantages les gouvernements fédéral, provinciaux, territoriaux et municipaux peuvent-ils attendre d'un investissement dans des centres de données ?*

Une fois construits, les centres de données requièrent très peu d'employé·es et contribuent très peu à l'économie. Par contre, ils nécessitent que les sociétés d'État qui produisent de l'énergie investissent dans une production accrue, ce qui entraîne une augmentation du coût de l'énergie pour l'ensemble de la population. Pourtant, des investissements essentiels en éducation, santé, logements sociaux font défaut. L'État devrait seulement soutenir l'installation de centres de données qui s'inscrivent dans une stratégie de souveraineté numérique, à des fins de bien commun.

5. Droits des peuples autochtones

> *(a) Comment les questions liées à l'IA influent-elles sur les systèmes juridiques autochtones, les connaissances traditionnelles, les droits fonciers et les titres fonciers, le droit à l'autonomie gouvernementale et la souveraineté numérique et des données des Autochtones (y compris les principes de propriété, de contrôle, d'accès et de possession [OCAP]) ?*

La souveraineté numérique est l'un des enjeux du droit à l'autodétermination des peuples autochtones. Comme l'affirme l'Assemblée des Premières Nations Québec-Labrador : « Les projets technologiques

doivent contribuer au renforcement des capacités des Premières Nations et soutenir un développement durable respectant leurs aspirations. »[40]

Le droit à l'autodétermination passe, entre autres, par le contrôle autochtone sur leurs institutions en santé, en éducation, en matière de sécurité publique, etc. Ce contrôle ne peut se faire sans une maîtrise des données concernant leurs propres populations. **En s'outillant pour atteindre la souveraineté numérique des populations allochtones, les gouvernements du Canada et du Québec devraient collaborer avec les peuples autochtones afin qu'ils puissent se doter des mêmes capacités.**

Le développement de l'IA se fait en s'appropriant toutes les données et savoirs accessibles sans égard aux droits des producteurs de ces données et savoirs. L'IA accentue le problème déjà existant du droit de propriété intellectuelle. Les grandes corporations utilisent ce « droit » pour s'approprier et monopoliser des connaissances et des substances (comme les semences) produites par d'autres en les brevetant. Les paysans et les peuples autochtones, qui sont souvent les mêmes personnes, sont particulièrement visés par ces pratiques. **Elles devraient être illégales. Les peuples autochtones, comme les autres titulaires de droits de propriété intellectuelle, devraient pouvoir déterminer les usages qui peuvent être de leurs savoirs et de leurs données et recevoir de justes redevances pour leur utilisation.**

> *(b) Que faut-il faire pour garantir que toute « stratégie nationale en matière d'IA » du Canada respecte les obligations du pays en vertu des traités préexistants, adhère à la Déclaration des Nations Unies sur les droits des peuples autochtones (DNUDPA) et fasse progresser les 94 appels à l'action issus de la Commission de vérité et réconciliation ?*

Le développement effréné de l'IA accentue la ruée vers les minéraux critiques et accroît les besoins énergétiques. Tant les mines que les infrastructures énergétiques -- pipelines, lignes de transmission électriques, barrages, éoliennes -- se situent souvent sur des territoires autochtones. L'impact de ces projets n'est pas seulement environnemental. Il est également social. L'établissement de camps miniers avec des travailleurs mobiles (fly in – fly out) peut avoir des effets délétères sur les communautés autochtones avoisinantes. L'accès aux emplois créés est aussi un enjeu. **Cela exige, plus que jamais, le respect du consentement préalable, libre et éclairé, prévu par la DNUDPA et le droit des peuples autochtones de dire NON.**

6. Égalité réelle, discrimination et oppression motivée par la haine

> *(a) Quelle est la prévalence de la discrimination facilitée par l'IA ou algorithmique fondée sur des catégories protégées, telles que la race, le sexe et l'âge ? Cette discrimination est-elle plus prononcée dans certains secteurs que dans d'autres ? Si oui, lesquels ?*
>
> *(b) Plus précisément, comment l'utilisation ou le déploiement de l'IA favorise-t-il ou compromet-il l'égalité des sexes, la justice raciale, l'égalité socio-économique, l'égalité en matière*

[40] Territoire numérique des Premières Nations Québec-Labrador: https://files.cssspnql.com/s/mUJuMtxNuTNS5Hc

d'orientation sexuelle et d'identité de genre, les droits des personnes handicapées ou la justice pour les migrants et les réfugiés ?

(c) Existe-t-il des cas de discrimination facilitée par l'IA ou algorithmique qui sont difficiles à identifier ou à mesurer lorsqu'ils se produisent ? Quels sont-ils et que peut-on faire pour y remédier et lutter contre leur invisibilité ?

Tout d'abord, nous tenons à souligner que l'égalité réelle n'implique pas nécessairement un traitement différencié entre différents groupes. L'analyse de l'égalité réelle peut exiger un traitement identique tout comme un traitement différent : c'est l'effet réel de la mesure qui doit être analysé en tenant compte des facteurs sociaux et historiques en lien avec le groupe. L'analyse, qui se transpose en contexte algorithmique, peut donc « démontrer qu'un traitement différent est discriminatoire en raison de son effet préjudiciable ou de l'application d'un stéréotype négatif ou, au contraire, qu'il est nécessaire pour améliorer la situation véritable du groupe de demandeurs[41] ».

La discrimination algorithmique est très prévalente dans puisque les systèmes d'IA ont souvent comme objectif d'effectuer des distinctions en se basant sur certaines caractéristiques[42] : « the very point of data mining is to provide a rational basis upon which to distinguish between individuals[43] ». Bien qu'il existe des cas où les SIA ont effectué des distinctions explicitement sur des motifs de discrimination (pensons aux publicités ciblées de Facebook qui pouvaient être choisies en fonction de l'âge et autres motifs), la grande majorité des cas de discrimination algorithmique réfèrent plutôt à des cas de discrimination indirecte. Ce sont eux qui sont plus difficiles à identifier ou à mesurer lorsqu'ils se produisent. Afin de comprendre ce phénomène, il importe de comprendre ce qui le cause. **Les SIA peuvent produire des résultats discriminatoires en raison de problèmes dans les données qui les alimentent et des choix des concepteur.trices**. D'abord, si certains groupes sont sous-représentés dans les données d'entraînement (pensons à un système de reconnaissance faciale entraîné sur une banque de données de visages avec un faible pourcentage de personnes racisées), le système apprendra moins bien à les reconnaître et donc comportera plus de failles à l'égard de personnes racisées. À l'inverse, une surreprésentation peut aussi causer des problèmes : les communautés marginalisées, soumises à une surveillance policière accrue, se retrouvent surreprésentées dans les données criminelles ou d'interpellation, ce qui amène les algorithmes prédictifs à les cibler davantage, créant un cercle vicieux autorenforçant. Par ailleurs, les données peuvent parfois ne pas contenir de problème de représentation, mais tout de même refléter des inégalités historiques et systémiques en lien avec des motifs de discrimination. Ainsi, l'A entraînée sur des données « exactes et représentatives » sur les personnes fait en sorte que ce SIA va reproduire et parfois amplifier ces mêmes inégalités.

À ces problèmes de données s'ajoutent des causes liées aux personnes qui conçoivent ces systèmes et aux objectifs qui leur sont assignés. Les équipes de développement en IA sont majoritairement non diversifiées, ce qui influence les choix de conception et peut aggraver les biais envers les groupes

---

[41] *Withler c. Canada (Procureur général), 2011 CSC 12*, para 39.

[42] Brian d'Alessandro, Cathy O'Neil et Tom LaGatta, « Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification » (2017) 5:2 Big Data à la p 121; West, Sarah Myers, Meredith Whittaker & Kate Crawford, *Discriminating systems: Gender, race and power in AI*, AINow Institute, 2019 à la p 6; Solon Barocas et Andrew D Selbst, « Big Data's Disparate Impact » (2016) 104:3 Cal L Rev à la p 677.

[43] Solon Barocas et Andrew D Selbst, « Big Data's Disparate Impact » (2016) 104:3 Cal L Rev à la p 677.

qu'elles connaissent moins bien. Enfin, la discrimination peut être intégrée dès le départ dans la finalité même du système : un outil conçu pour détecter la fraude uniquement chez les personnes défavorisées, comme ce fut le cas aux Pays-Bas avec le système SYRI[44] ou en Australie avec Robo-debt[45], pose un problème de discrimination par défaut. En effet, « lorsque l'objectif d'un modèle d'apprentissage automatique s'accorde mal avec la nécessité d'éviter la discrimination, les résultats qu'il produit perpétueront ou exacerberont à nouveau celle-ci »[46].

7. Bien-être mental, social et cognitif

> *(a) Quels problèmes cognitifs, de santé mentale ou psychologiques découlent de certaines utilisations de l'IA ou de son utilisation par certains groupes vulnérables (par exemple, les enfants, les lycéens, les personnes âgées) dans certaines circonstances (par exemple, conversations quotidiennes prolongées avec un chatbot flagorneur tel que ChatGPT, externalisation de tâches cognitives de base et de la pensée critique) ?*

Les effets délétères des longues heures passées devant les écrans et des interactions avec de grands modèles de langage (Large language models) sur la socialisation et le développement cognitif des jeunes sont de plus en plus documentés. De plus en plus de juridictions limitent l'accès des jeunes aux écrans (interdiction des téléphones à l'école) et aux réseaux sociaux (interdiction avant un certain âge). Tant que ces outils seront sous le contrôle d'intérêts privés conçus pour créer des dépendances sans égard aux conséquences et sans régulation efficace, de telles interdictions deviennent inévitables. Au Québec et au Canada, la tâche de protéger les jeunes est essentiellement laissée aux parents. La déresponsabilisation des entreprises et de l'État est inacceptable. **Une réglementation protégeant les jeunes et respectueuse du droit à la vie privée est nécessaire.**

> *(b) Comment les personnes ou les entreprises déploient-elles l'IA de manière à manipuler les gens ou à compromettre ou déformer l'action humaine ? Que faut-il faire?*

Les données comportementales récoltées peuvent tout aussi bien être utilisées pour influencer nos habitudes de consommation que des processus démocratiques, comme les référendums et les élections. Le cas de Cambridge Analytica, qui est intervenu pour influencer les élections de 2016 aux États-Unis et le vote sur la sortie du Royaume-Uni de l'Union européenne, le Brexit, est bien documenté.

Le fonctionnement même des plateformes contribue à polluer le débat démocratique. Pour mousser l'engagement de l'internaute, les plateformes mettent à l'avant-plan les « nouvelles » les plus sensationnalistes et, par le fait même se trouvent à faire la promotion des fake news. Pour maintenir

---

[44] Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, *Rapport d'Amicus Curiae*, NJCM et al. v The Dutch State (case number: C/09/550982/ HAZA 18/388) à la p 9.

[45] Achiume, E. Tendayi, *Discrimination raciale et nouvelles technologies numériques : analyse sous l'angle des droits de l'homme*, Rapport de la Rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Doc off AG NU, Conseil des droits de l'homme, 44e sess, Doc NU A/HRC/44/57.

[46] Lacroix, Christophe, *Prévenir les discriminations résultant de l'utilisation de l'intelligence artificielle,* Commission sur l'égalité et la non-discrimination, Conseil de l'Europe, Doc 15151, 2020, à la p 14.

son intérêt, elles vont proposer des liens vers des sites qui confortent ses opinions, le confinant dans des chambres d'écho qui favorisent la montée aux extrêmes.

En donnant accès à des millions de personnes à des influenceurs comme Andrew Tates et Nick Fuentes, les plateformes jouent aussi un rôle important dans la pénétration du suprémacisme blanc et du masculinisme dans la jeunesse.

8. Médecine et soins de santé

> *(a) Quels sont les avantages et les inconvénients liés à l'utilisation de certains types d'IA dans les soins médicaux, la recherche médicale, les dispositifs médicaux et les soins infirmiers ?*
>
> *(b) Comment atténuer ou prévenir les risques, les problèmes et les conséquences négatives liés à l'utilisation de l'IA dans les applications liées à la santé ?*

Dans un contexte de difficulté d'accès à des professionnel·les de la santé, de plus en plus de personnes ont recours à de grands modèles de langage pour des conseils relatifs à des problèmes de santé, tant physiques que mentaux. Alors que les professionnel·les de la santé ont suivi une formation accréditée et sont soumis à des contrôles, ces modèles opèrent de manière opaque, sans contrôle externe et sans responsabilité des entreprises. Les conseils prodigués peuvent être erronés ou même dangereux. **De tels outils peuvent être utiles, mais seulement s'ils sont validés par des professionnels compétents, ce qui n'est pas le cas présentement.**

Par ailleurs, la discrimination algorithmique constitue un risque aussi dans les applications d'IA en santé. Par exemple, des systèmes d'IA utilisés en dermatologie pour détecter les mélanomes sont moins performants auprès des personnes racisées, dont la peau est sous-représentée dans les données d'entraînement. Cela soulève que lorsqu'on aborde les bienfaits des outils d'IA en santé, il faut porter une attention à qui est exclu de ces bienfaits.

9. Enfants et jeunes

> *(a) Existe-t-il des utilisations ou des déploiements de l'IA auxquels les enfants ou les adolescents sont particulièrement vulnérables ou sensibles ? Quels sont-ils et pourquoi ?*

Les plateformes sont fondées sur la base d'une rétroaction conçue pour développer une dépendance aux écrans, ce qui entraîne des effets délétères sur la santé. **Elles peuvent favoriser l'isolement au détriment de rapports sociaux significatifs.** L'impact est particulièrement toxique pour les jeunes, affectant les filles de manière disproportionnée, augmentant leurs troubles alimentaires et pensées

suicidaires. Dans sa dénonciation de Facebook, la lanceuse d'alerte Frances Haugen a dévoilé des études internes de Facebook qui montraient que la compagnie était au courant de ces effets[47].

10. Justice, application de la loi et sécurité nationale

(a) Quels sont les principaux enjeux et implications liés à l'utilisation de l'IA dans les domaines de l'application de la loi, de la justice pénale, du renseignement et de la sécurité nationale ?

Au Canada, plusieurs corps policiers expérimentent avec l'IA d'une manière opaque et en l'absence d'encadrement législatif suffisant. La GRC a utilisé Clearview AI en violation de la *Loi sur la protection des renseignements personnels*[48], et plusieurs services policiers, dont ceux de Vancouver, Calgary, Edmonton, Toronto et Saskatoon, ont recours à des outils de police prédictive[49]. Comme le souligne le rapport du Citizen Lab, ces systèmes reproduisent et amplifient les biais systémiques existants, notamment en ciblant les communautés racisées et marginalisées déjà soumises à une surveillance policière accrue[50].

Au Québec, le SPVM a acquis en 2025 un logiciel d'IA d'analyse vidéo au coût de 1,8 M$ permettant de rechercher une personne selon son habillement ou un véhicule par sa plaque. Le SPVM refuse de dévoiler le nom du logiciel et il soutient avoir réalisé une « Évaluation des facteurs relatifs à la vie privée », mais refuse également de rendre ce document public[51]. Ce manque de transparence est représentatif : les corps policiers canadiens ont à plusieurs reprises dissimulé ou minimisé leur recours à ces technologies, comme l'a illustré de façon flagrante la GRC, qui a d'abord nié utiliser Clearview AI avant d'admettre s'en être servie dans diverses d'enquêtes, pour des fins qui demeurent en grande partie inexpliquées, 85% des recherches effectuées n'ayant pas été justifiées auprès du Commissariat à la protection de la vie privée du Canada[52]. Ainsi, « [t]his type of intentional opacity represents a challenge since many individuals will not even be aware they've been subjected to AI systems »[53],

---

[47] Bobby Allyn, Here are 4 key points from the Facebook whistle blower's testimony on Capitol Hill, National Public Radio, octobre 2021, https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress

[48] Commissariat à la protection de la vie privée du Canada, Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée, 2021, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/

[49] Kate Robertson, Cynthia Khoo et Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*, Citizen Lab, 2020, https://citizenlab.ca/research/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

[50] Ibid.

[51] William Thériault, Le SPVM sera soutenu par l'intelligence artificielle, La Presse, 2025, https://www.lapresse.ca/actualites/justice-et-faits-divers/2025-10-06/logiciel-d-analyse-video/le-spvm-sera-soutenu-par-l-intelligence-artificielle.php; Nora Lamontagne, La police de Montréal peut maintenant vous surveiller en temps réel avec l'IA, Journal de Montréal, 2025, https://www.journaldemontreal.com/2026/01/10/le-spvm-peut-maintenant-vous-surveiller-en-temps-reel-avec-lia#cxrecs_s.

[52] Commissariat à la protection de la vie privée du Canada, Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée, 2021, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/

[53] Lucia Flores Echaiz, "Artificial Intelligence in Canada and Equality: Algorithmic Discrimination and Section 15(1) of the Charter" dans *Cant Compute: Moving Towards an Equitable Digital World,* https://ruor.uottawa.ca/server/api/core/bitstreams/14d62074-536d-435e-97c6-90f0375f6482/content, à la p. 111.

soulignant un enjeu préalable à tous les autres, puisque sans transparence, l'accès à la justice est compromis.

L'utilisation de l'IA par la police, que ce soit par le recours à des systèmes de police prédictive ou de reconnaissance faciale, soulève de graves inquiétudes en lien avec le droit à l'égalité, le droit à la vie privée, mais également en cas d'interception policière basée sur ces outils, à l'égard du droit contre les fouilles abusives et le droit contre la détention arbitraire.

Aussi, le déploiement des systèmes de reconnaissance faciale dans l'espace public à des fins d'application de la loi soulève de grandes inquiétudes sur l'effet paralysant que cette surveillance exerce sur les libertés d'expression, d'association et de réunion pacifique.

Selon la LDL, la surveillance de masse des lieux et endroits publics au moyen de la reconnaissance faciale doit formellement être interdite[54]. La surveillance de masse en ligne par les services policiers, notamment sur les réseaux sociaux, doit également être proscrite, les services policiers ne devant pas recueillir des images sur Internet pour les soumettre à des systèmes de reconnaissance faciale[55]. Enfin, les services policiers doivent être interdits d'utiliser des outils de reconnaissance faciale sur les banques d'images constituées par les organismes publics ou ministères dans l'exercice de leurs mandats, tels que les photos de permis de conduire ou passeports[56].

De plus, pour la LDL, un moratoire s'impose sur toute autre utilisation de la reconnaissance faciale par les services policiers ainsi que sur l'utilisation d'outils de police prédictive, et ce, jusqu'à l'adoption d'une législation à la mesure des enjeux, fondée sur un débat public informé et transparent.

12. Confidentialité et protection des données

> *(a) Quels sont les enjeux et les implications en matière de confidentialité, de protection des données et de surveillance liés à l'utilisation de l'IA par les particuliers, les gouvernements et/ou les entreprises ?*

Sans mesures de sécurité déployées à grande échelle en matière de confidentialité, de protection des données et de surveillance, le tsunami de l'IA représente une menace extrême : le séisme pourrait être tel qu'il emportera dans son sillage le **droit à la vie privée**, enchâssé dans les chartes québécoise et canadienne.

Les lois actuelles sur la protection des renseignements personnels[57] en vigueur tant au niveau provincial que fédéral, ne sont pas à la hauteur dans le contexte du développement effréné de l'IA.

---

[54] Ligue des droits et libertés, *Consultation sur le Document d'orientation préliminaire sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, 2021, https://liguedesdroits.ca/wp-content/fichiers/2021/10/memoire_ldl_orientations_rf_cpvp_cai_20211015.pdf

[55] Ibid.

[56] Ibid.

[57] Québec : Loi sur la protection des renseignements personnels dans le secteur privé (modernisé par la loi 25) : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/fr/2021/2021C25F.PDF

Les gouvernements ont la responsabilité d'adopter des législations robustes afin d'assurer le respect et la protection du droit à la vie privée, tant par et au sein de l'État que par les entreprises et les organisations.

Or, les experts sonnent l'alarme, rappelant que « [...] notre droit au respect de la vie privée est menacé à différentes étapes du processus : cueillette des données, analyse, évaluation des résultats. »[58]

Les menaces liées à l'IA sont aussi nombreuses que l'utilisation qui en est faite *:* « Le siphonnage massif de données sur les réseaux sociaux, la reconnaissance faciale, l'Internet des objets, les systèmes de localisation GPS, les drones dopés à l'IA, les capteurs de données des villes intelligentes, les assistants vocaux au nom rassurant : tout cet attirail d'encerclement se développe sans contrôle ni débat public et paraît en voie d'anéantir toute possibilité de vie privée, en plus de mettre à mal de nombreux autres droits humains »[59].

(b) Comment ces risques peuvent-ils être atténués, ou peuvent-ils l'être ?

Plusieurs pistes d'actions concertées seraient nécessaires, notamment :

- **Protéger le droit à la vie privée :** Il est nécessaire de placer le droit à la vie privée en amont et au cœur de tout projet lié à l'IA au sein des institutions publiques ou privées, plutôt que de l'asservir à l'industrie.
- **Protéger les personnes en situation de vulnérabilité :** Les personnes en situation de vulnérabilité, dont les enfants, sont particulièrement à risque.
- **Interdire la surveillance massive de la population par les entreprises et par l'État :** Qu'elle soit à des fins de sécurité, ou pour des visées politiques ou commerciales, la surveillance massive doit être fermement interdite.
- **Solliciter la participation de la société civile :** Les transformations et les utilisations à venir doivent être transparentes et compréhensibles. La population doit être informée et consultée au regard des produits qui utilisent ses données personnelles.
- **Maintenir une vigie continue et une imputabilité :** Des audits doivent permettre d'éviter les risques de dérive quant à la confidentialité et la protection des données personnelles. L'organisation elle-même ainsi que des responsables identifiés doivent être imputables advenant un bris de confidentialité.

---

https://www.legisquebec.gouv.qc.ca/fr/document/lc/p-39.1
Institutions du gouvernement fédéral : Loi sur la protection des renseignements personnels : https://laws-lois.justice.gc.ca/FRA/LOIS/P-21/index.html
Loi fédérale sur la protection des renseignements personnels et les documents électroniques - secteur privé : https://laws-lois.justice.gc.ca/fra/lois/P-8.6/page-2.html#h-6

[58] Riezebos, S., Gelissen, T., Saxena R. (2023). Démocratiser l'élaboration de politiques en matière d'IA dans *Supervision humaine et imputabilité : Angles morts de la gouvernance de l'IA (Ouvrage collectif)* (p. 322) UNESCO et MILA
https://unesdoc.unesco.org/ark:/48223/pf0000384801

[59] Pineau, A. (2020). Assujettir l'intelligence artificielle au respect de la vie privée et des droits humains. *Droits et libertés,* https://liguedesdroits.ca/chronique-surveillance-ia/

- **Assurer l'étanchéité entre les systèmes :** Les programmes de l'IA ayant recours à des données personnelles autorisées doivent être étanches l'un de l'autre afin d'empêcher les recoupements permettant d'établir un profil complet de l'individu violant ainsi le respect de sa vie privée.
- **Éduquer et sensibiliser :** L'éducation de la population aux risques de l'IA sur la vie privée et aux mesures à prendre pour protéger ses renseignements personnels est essentielle.
- **Assurer le respect du consentement :** Voir la section suivante.

13. Consentement

(a) Dans quelles circonstances, cas d'utilisation ou déploiements le consentement est-il une mesure efficace pour réglementer et prévenir les effets néfastes de l'IA ? Dans quelles circonstances, cas d'utilisation ou déploiement le consentement est-il moins efficace ou inefficace en tant que mesure ? Quels sont les facteurs qui déterminent l'efficacité ou non du consentement en tant que mécanisme ?

(b) Existe-t-il des utilisations de l'IA qui devraient être interdites, que la ou les personnes concernées aient donné leur consentement ou non ? Si oui, lesquelles et pourquoi ?

(c) Compte tenu de la nature des systèmes d'IA, les utilisateurs, les consommateurs ou les personnes concernées peuvent-ils retirer leur consentement une fois qu'il a été donné ? Pourquoi ou pourquoi pas, et comment cela devrait-il influencer la législation et l'élaboration des politiques en matière d'IA ?

(d) Dans le contexte d'un système d'IA donné, que signifie le fait qu'une personne ait donné un consentement significatif, valide et éclairé ? Les exigences pour répondre à cette norme de consentement devraient-elles différer selon le groupe (par exemple, les enfants, les adolescents, les parents, les personnes âgées) ?

(e) Une personne devrait-elle pouvoir se désinscrire complètement des systèmes d'IA si elle le souhaite, ou dans quelles circonstances ou cas d'utilisation ? Quels sont les avantages ou les inconvénients d'un système d'adhésion volontaire par rapport à un système de désinscription (tel que celui qui a été appliqué dans le contexte de la protection de la vie privée et des données) ? Que faudrait-il pour mettre en place un système d'adhésion ou de désengagement universel unique pour les consommateurs ou les personnes concernées par un système d'IA donné ? La loi devrait-elle exiger que cette option soit offerte aux personnes (par exemple, dans les appareils électroniques, dans les décisions concernant des intérêts juridiques ou similaires importants, dans les salles de classe) ?

Les lois de protection des renseignements personnels (RP) ont comme pierre d'assise le « consentement ». Or, ce concept fait fi de l'inégalité des parties en présence. Quel pouvoir les individus ont-ils réellement de refuser l'accès à leurs données s'ils veulent accéder aux services disponibles sur le Net? Pratiquement aucun. Certes on peut à l'occasion refuser certains cookies mais la négociation est rarement possible quant aux conditions d'utilisation des réseaux sociaux, plateformes numériques et autres outils des géants du Web; sans compter les objets connectés.

Au Québec, les récentes modifications apportées aux lois (publique et privée) de protection des RP (Loi 25) demeurent cosmétiques. Elles exigent le consentement à la cueillette de RP tout en énumérant

une série d'exceptions. La procédure de consentement n'est pas standardisée; elle varie d'une entreprise à l'autre; elle est parfois laborieuse (nombreuses cases à cocher) ou ambigüe (doit-on cocher ou décocher?); et vise souvent à tromper ou du moins à décourager les refus de cueillette de données.

Ces modifications législatives ne s'attaquent pas au déséquilibre des forces en présence et laissent dans l'ombre des enjeux névralgiques, notamment l'illégitimité d'une industrie fondée sur la surveillance et l'appropriation des données personnelles. La longue inaction des gouvernements, tant ici que dans le reste du monde, a malheureusement permis le déploiement de modèles d'affaires liberticides, une « nouvelle forme de commerce dépendant de la surveillance en ligne à grande échelle »[60].

L'essor du modèle économique fondé sur la surveillance a conduit deux entreprises (Google et Facebook) à contrôler une architecture de surveillance sans précédent dans l'histoire de l'humanité. Le modèle économique fondé sur la surveillance est incompatible avec le droit à la vie privée et constitue une menace grave pour une série d'autres droits humains.

Les géants du Web (GAFAM : Google, Apple, Facebook, Amazon, Microsoft) ne sont du reste plus seuls sur la patinoire; de nombreuses autres entreprises adoptent aujourd'hui ce modèle d'affaires : (finances, banques, assurances, etc.) Cette logique de surveillance et d'extraction de données s'étend aussi au monde réel par le biais des objets connectés. Comme l'explique Soshana Zuboff :

> Tous les niveaux de notre vie personnelle sont automatiquement captés et comprimés en un flux de données à destination des chaînes de montage qui produisent de la certitude. Accomplie sous couvert de « personnalisation », une bonne part de ce travail consiste en une extraction intrusive des aspects les plus intimes de notre quotidien.[61]

Une industrie fondée sur l'espionnage de la population et l'appropriation des données résultant de ses activités, de ses pensées, de ses questionnements et de ses interactions est-elle légitime? Est-ce compatible avec le maintien d'une société libre et démocratique ? Nous ne le croyons pas.

Ce modèle d'affaires qui vampirise l'expérience humaine n'a fait l'objet d'aucune discussion ni débat public. Et le « consentement » des personnes à divulguer leurs RP ne doit pas servir à le cautionner. Comme l'indique le professeur Pierre Trudel :

> Encadrer les processus par lesquels on génère de la valeur avec les données en multipliant les obligations d'obtenir le « consentement » des individus pour utiliser des données ne suffit pas. Il faut rétablir la capacité des États à réguler les activités de cette société de capitalisme de surveillance. Il faut des lois qui déterminent les droits et les obligations des personnes, individus, entreprises et gouvernants dans la production de valeur à partir des données[62].

---

[60] https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443

[61] https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443

[62] https://www.ledevoir.com/opinion/chroniques/722499/chronique-nos-donnees-expropriees

Un chantier de réflexion s'impose sur cette nouvelle économie des données. Tout comme un encadrement robuste s'impose dans l'utilisation de l'intelligence artificielle. Le fonctionnement des algorithmes utilisés par l'État et l'entreprise privée doit être divulgué publiquement en vue d'en contrôler l'utilisation et les biais. Des garanties de loyauté, de transparence et de reddition de comptes doivent s'appliquer à l'exploitation de tels systèmes d'intelligence artificielle.

14. Droits constitutionnels, droits humains et démocratie

Nous avons abordé les enjeux relatifs aux droits humains dans l'ensemble du document.

18. « Souveraineté » numérique et IA

> *(a) Une grande partie de la vague actuelle d'investissements exceptionnellement importants dans l'IA est le fait d'entreprises et de gouvernements de grands pays autres que le Canada, qui consolident ainsi leur propre pouvoir et acquièrent un plus grand contrôle sur l'avenir de l'IA dans leur juridiction. Quelles sont les implications pour les intérêts nationaux et la souveraineté du Canada ? Que devrait faire le gouvernement canadien à cet égard ?*
>
> *(b) Comment définiriez-vous la « souveraineté en matière d'IA » ou la « souveraineté numérique » ? S'agit-il d'un concept utile pour orienter la législation, les politiques, la réglementation et/ou la gouvernance canadiennes en matière d'IA, et pourquoi ?*

La souveraineté numérique est un principe juridique selon lequel les données doivent être soumises aux lois et réglementations du pays où elles ont été produites, traitées ou stockées, et qui contribue notamment à la protection des informations sensibles d'un État ainsi qu'à leur utilisation éthique.

La souveraineté numérique concerne tant l'hébergement et le traitement des données que l'utilisation de logiciels et outils numériques libres pour parvenir à se sortir de la dépendance envers les entreprises étrangères et privées.

En février 2026, le gouvernement du Québec a rendu public un « Énoncé de politique de souveraineté numérique et d'approvisionnement en technologie de l'information[63] » dans lequel il propose une définition de la souveraineté numérique[64], mais qui demeure à l'heure actuelle au stade de simple énoncé. Plusieurs actions gouvernementales demeurent en contradiction avec ces principes, notamment le projet Dossier santé numérique, qui serait confié à l'entreprise états-unienne Epic Systems[65].

---

[63] https://www.quebec.ca/gouvernement/numerique/souverainete-numerique

[64] « La souveraineté numérique désigne la capacité pour un gouvernement de contrôler et de protéger ses infrastructures numériques, ses technologies et ses données contre les influences étrangères en s'assurant notamment que les lois prises dans un autre pays ne peuvent s'appliquer. Elle vise ainsi à réduire la dépendance d'un gouvernement envers des entreprises étrangères.Elle englobe la gestion sécurisée des informations, la protection des renseignements personnels contre tout accès non autorisé et la confidentialité des échanges numériques. »

[65] https://ici.radio-canada.ca/nouvelle/2239638/dossier-sante-numerique-epic-systems

De son côté, la Ligue des droits et libertés en collaboration avec d'autres organisations de la société civile – Co-Savoir; FACiL, pour l'appropriation collective de l'informatique libre; le Syndicat de la fonction publique et parapublique du Québec (SFPQ); et le Syndicat de professionnelles et professionnels du gouvernement du Québec (SPGQ) – a lancé en juin 2025 une campagne sur la souveraineté numérique, appelant le gouvernement du Québec à mettre fin à la sous-traitance des données des Québécois-es à des entreprises privées, souvent états-uniennes.[66]

Actuellement, le gouvernement du Québec sous-traite à des entreprises privées, très souvent américaines, l'hébergement en infonuagique des données qu'il détient sur la population, les ressources naturelles et les infrastructures.

Nous demandons au gouvernement du Québec de reprendre le contrôle sur l'hébergement de nos données en garantissant une gestion transparente et sécuritaire qui protège les droits humains, particulièrement les droits à la vie privée et à la sécurité.

Le gouvernement doit mettre fin à la sous-traitance démesurée au privé et développer, dès maintenant, ses propres infrastructures d'hébergement de données, en priorisant les logiciels libres, pour favoriser une souveraineté numérique populaire et pas seulement étatique. Il doit aussi rapatrier l'expertise nécessaire à la gestion des données au sein du gouvernement.

En ce qui concerne plus spécifiquement la souveraineté en matière d'IA, celle-ci implique tant l'hébergement des données que le développement des modèles d'IA et le traitement des données. Elle implique de développer des compétences propres, de construire des systèmes d'IA qui respectent le cadre juridique canadien et québécois et d'avoir un contrôle sur ces systèmes, plutôt que de sous-traiter ces capacités à des entreprises étrangères dont les intérêts ne correspondent pas nécessairement à ceux de la population.

20. Lutter contre la discrimination algorithmique

> *(a) Comment le gouvernement, les régulateurs, les développeurs de technologies ou les utilisateurs d'outils d'IA (par exemple, les employeurs, les propriétaires immobiliers, les banques) devraient-ils traiter cette discrimination algorithmique ? Comment la discrimination peut-elle ou doit-elle être identifiée ou gérée sur la base de critères indirects pour les catégories protégées ? Comment la discrimination doit-elle être analysée et prise en compte dans une perspective intersectionnelle, lorsque plusieurs catégories protégées sont impliquées pour un même individu ou une même communauté ?*
>
> *(c) Faut-il créer de nouvelles lois pour lutter contre la discrimination algorithmique, et comment ces lois interagiraient-elles avec les lois existantes qui traitent de la discrimination dans des domaines tels que le logement, l'emploi, le travail et l'éducation ? Faut-il adopter différentes lois traitant de la discrimination algorithmique au sein de secteurs spécifiques et adaptés à ceux-ci, ou faut-il adopter une législation globale qui s'applique à tous les secteurs ?*

[66] https://liguedesdroits.ca/souverainete-numerique-quebec-reprenons-le-controle-de-nos-donnees/

En principe, la conception de l'égalité réelle au cœur de la protection du droit à l'égalité prévu dans les Chartes canadienne et québécoise est adaptée pour appréhender la discrimination algorithmique, puisque l'égalité réelle s'intéresse à l'effet réel des mesures (et non à l'intention), aux injustices historiques et systémiques. Elle reconnaît qu'il n'est pas nécessaire que toutes les personnes d'un groupe soient visées de la même façon par la mesure contestée et permet les motifs intercroisés (l'analyse intersectionnelle) - tous des éléments pertinents en contexte de discrimination issue des systèmes d'IA[67].

Toutefois, au niveau de l'application jurisprudentielle, il existe des tensions importantes, diminuant potentiellement la portée de la protection du droit à l'égalité à l'égard de la discrimination algorithmique[68]. Depuis l'arrêt *Ward,* le seuil élevé d'atteinte à la dignité risque de constituer un obstacle important dans les recours en discrimination algorithmique[69]. De plus, *Sharma* introduit le caractère non arbitraire de la distinction comme facteur pertinent dans l'analyse, ce qui pourrait nuire aux plaignant·es dans un contexte algorithmique où les systèmes d'IA sont précisément présentés comme rationnels et objectifs[70]. Sharma renforce par ailleurs une interprétation restrictive de l'analyse de l'article 15(1) de la *Charte canadienne* qui pourrait imposer indûment aux plaignant·es de prouver une aggravation du désavantage causé par le système d'IA en question plutôt que sa simple reconduction[71].

Compte tenu de ces tensions dans l'analyse du droit à l'égalité, une ou plusieurs législations spécifiques pourraient être utiles pour permettre la concrétisation des principes de l'égalité réelle. En effet, bien que la discrimination algorithmique soit déjà interdite par les chartes, il serait intéressant de l'interdire explicitement et d'imposer des obligations de transparence et d'accès à l'information permettant de surmonter les problèmes d'opacité entourant les systèmes d'IA – qui représentent des obstacles préalables dans l'accès à la justice. L'objectif ne serait pas de supplanter les chartes, mais de créer des obligations concrètes contre la discrimination algorithmique, ce qui pourrait d'ailleurs influencer positivement les tribunaux dans l'interprétation qu'ils feraient du droit à l'égalité dans des recours en discrimination algorithmique fondés sur les chartes.

D'ailleurs, l'interdiction de la discrimination algorithmique et les moyens pour lutter ce problème concerne tous les acteurs : les gouvernements, régulateurs, développeurs et institutions qui déploient les systèmes d'IA, dont les employeurs, propriétaires et institutions financières. Tous ont la responsabilité de s'assurer que les systèmes d'IA qu'ils conçoivent ou utilisent respectent les principes de l'égalité réelle. Cela implique notamment qu'un développeur ne peut se décharger de sa responsabilité en démontrant que son système satisfait à une métrique d'équité algorithmique fondée sur une conception formelle de l'égalité ou conforme au cadre juridique d'un autre pays : c'est l'égalité

---

[67] Flores Echaiz, Lucia (2025). « Le droit à l'égalité canadien et québécois face à la discrimination algorithmique » Mémoire. Montréal (Québec, Canada), Université du Québec à Montréal, https://archipel.uqam.ca/18854/1/M19074.pdf aux pp 126-135.

[68] *Ibid* aux pp 151-155, 163-164 et 170.

[69] *Ibid* aux pp 163-164. Voir *Ward c. Québec (Commission des droits de la personne et des droits de la jeunesse)*, 2021 CSC 43.

[70] *Ibid* aux pp 151-155. Voir *R. c. Sharma,* 2022 CSC 39.

[71] *Ibid.*

réelle, telle qu'interprétée de façon large et libérale en droit canadien et québécois, qui constitue le cade pertinent.

> *(d) Devrait-il y avoir une exemption dans les lois sur la discrimination algorithmique pour les systèmes qui différencient et ciblent différents groupes afin d'atténuer la discrimination historique et systémique (par exemple, les programmes d'action positive) ? Comment une telle exemption fonctionnerait-elle et qu'est-ce qui l'empêcherait de permettre une discrimination interdite ?*

Sur la question de la discrimination positive, la *Charte canadienne* et la *Charte québécoise* prévoient que les programmes correcteurs des inégalités ne constituent pas de la discrimination. Ainsi, a priori, un système d'IA conçu pour atténuer des désavantages historiques pourrait être légitime, mais cela ne saurait être présumé uniquement en fonction de l'objectif déclaré. L'égalité réelle ne s'intéresse pas aux intentions : c'est l'effet réel du système qui doit être évalué, et un outil présenté comme correcteur pourrait tout de même produire des effets discriminatoires à la lumière de l'égalité réelle.

21. Réglementation et législation en matière d'IA

Selon Max Tegmark, professeur au Massachusetts Institute of Technology, « la situation actuelle en matière d'IA est vraiment démentielle. **Aux États-Unis et au Canada, l'IA est moins réglementée que les sandwichs** »[72]. Et pourtant, les robots conversationnels ont déjà fait des centaines de victimes parmi les enfants (suicides, psychoses, etc.). Une telle approche n'est pas apte à renforcer la confiance des citoyens.

Les lois de protection des renseignements personnels (fédérales ou provinciales) s'avèrent toujours aussi inadéquates dans le contexte du développement effréné de l'IA. Et un vide juridique subsiste en ce qui concerne l'encadrement du développement et de l'utilisation de l'IA.

La LDL s'est exprimée à de nombreuses reprises pour exiger, comme d'autres, des législations et cadres réglementaires robustes pouvant réguler l'industrie de l'IA à des fins de bien commun et pour assurer la protection des droits humains.

> *(a) Quels enseignements le gouvernement fédéral devrait-il tirer des approches précédentes, des échecs et des leçons apprises lors des précédents changements sociétaux majeurs et cycles de hype technologique, qu'il s'agisse de l'Internet sans fil, du bug de l'an 2000, des smartphones, du « big data », des réseaux sociaux, des nouveaux médias ou des plateformes numériques ?*

[72] Tegmark, M., professeur, MIT, Future of Life Institute, Comité permanent de l'accès à l'information, de la protection de la vie privée et de l'éthique, 2 février 2025, https://www.ourcommons.ca/DocumentViewer/fr/45-1/ETHI/reunion-25/temoignages

Un exemple à rappeler, quoique dans un autre domaine, est celui de la crise financière des produits dérivés aux États-Unis en 2008. Ces produits financiers complexes ont détruit l'économie et la vie de millions d'Américains qui ont tout perdu. La réglementation qui régissait les banques et institutions financières avait auparavant été considérablement affaiblie. Et pourtant, ce sont les institutions financières responsables du désastre qui ont reçu l'aide de l'État, tandis que la population a assumé les coûts du « bail out ». Plusieurs font état aujourd'hui d'un risque d'une « bulle de l'IA » et craignent un scénario semblable avec les Big Tech.

Comme l'a noté très justement le Centre canadien de Politiques alternatives, l'argument selon lequel la réglementation de l'IA et la mise en place de garde-fous seraient contraires à l'innovation ne tient tout simplement pas la route. Bien au contraire :

> Historiquement, des cadres réglementaires clairs ont assuré la stabilité nécessaire à l'innovation. Les normes de sécurité dans les secteurs pharmaceutique, aéronautique et financier n'ont pas étouffé l'innovation ; elles l'ont orientée vers la confiance du public et la viabilité à long terme[73]".

> *(e) Y a-t-il des utilisations de l'IA qui devraient être purement et simplement interdites, et non simplement réglementées (à l'instar des « zones interdites » établies par le Commissariat à la protection de la vie privée du Canada ou des applications interdites par la loi européenne sur l'IA) ? Si oui, lesquelles et pourquoi ?*

La production d'applications, telles que celles qui permettent de dénuder des personnes, de créer de fausses images et vidéos pornographiques de personnes existantes ou du matériel pédopornographique devraient représenter une infraction dont les producteurs et les diffuseurs devraient être tenus responsables. Les créateurs d'IA doivent rendre de telles utilisations de leur logiciel impossible.

L'intégration de technologies avancées d'IA au domaine militaire, notamment l'usage des armes autonomes dans les guerres actuelles pour accélérer la « chaîne de destruction » ou séquence d'attaques, devraient être interdites, ou à tout le moins, strictement réglementée selon des critères éthiques, de sécurité, et de respect du droit international. La collecte de renseignements, la sélection puis les frappes de nombreuses cibles n'exigent plus que quelques secondes, si bien que la supervision humaine visant à en vérifier la légalité devient pratiquement impossible. Dans le cas d'erreurs, qui se comptent en victimes civiles, sinon en massacres de masse, la responsabilité devient plus difficile à établir. Comme l'affirme Heidi Khlaaf, la plupart des modèles d'IA utilisés par les militaires sont des « boîtes noires » dont le fonctionnement échappe à leurs utilisateurs[74].

---

[73] Pettigrew, R., Will Canada Govern AI for the Public Good? *Centre canadien de politiques alternatives*, 6 mars, 2026, https://www.policyalternatives.ca/news-research/will-canada-govern-ai-for-the-public-good/

[74] Gupta, D., En rationalisant la chaîne de destruction, l'IA transforme la guerre moderne, 23 mars 2026, France 24, https://fr.news.yahoo.com/rationnalisant-cha%C3%AEne-destruction-lia-transforme-135422458.html

(i) Quels sont les organismes gouvernementaux qui devraient être chargés de superviser et d'appliquer les lois et les règlements relatifs à l'IA, ou aux différentes utilisations et déploiements de l'IA?

En ce qui concerne la protection de la vie privée, nous sommes d'avis que la recommandation du Commissariat à la protection de la vie privée du Canada de se voir accorder des pouvoirs accrus d'exécution de la loi, le pouvoir d'émettre des ordonnances et d'imposer, lorsque nécessaire, des amendes, est entièrement justifiée[75]. Des ressources suffisantes permettant au bureau du Commissariat de réaliser pleinement son mandat doivent également être octroyées.

Le projet de loi C-27, mort au feuilleton en janvier 2025, qui comportait une section sur l'IA, proposait la création d'un commissaire à l'IA et aux données[76]. Nous sommes d'avis qu'un tel poste pourrait être intéressant, plus spécifiquement un commissaire à l'IA et aux droits humains. Toutefois, ce commissaire devrait disposer d'une véritable indépendance à l'égard de l'exécutif, et non être désigné par le ministre comme le prévoyait la LIAD, ainsi que de pouvoirs réels, tels qu'une capacité d'enquête, de décisions contraignantes et d'imposition de sanctions. Son mandat ne devrait pas inclure le fait de promouvoir le développement de l'IA, mais tout simplement de veiller au respect des droits humains en lien avec l'IA.

Conclusion

Il appert de ce qui précède que les technologies relevant de l'IA exerceront des impacts significatifs, parfois inquiétants, et possiblement irréversibles, sur les droits et libertés ainsi que sur l'intégrité de nos institutions démocratiques. La société civile est d'avis que **l'IA est un sujet bien trop grave pour être laissée entre les mains de quelques décideurs qui en détermineraient les orientations.**

La LDL salue l'initiative de consultation populaire sur l'IA et appelle les autorités gouvernementales à tenir compte des préoccupations formulées par la société civile. Il est clair que celle-ci favorise l'établissement d'une réglementation appropriée en matière d'IA, apte à susciter la confiance nécessaire au sain développement de ces technologies. Enfin, nous sommes confiants que cette réflexion approfondie viendra enrichir l'exercice de consultation tenu par le gouvernement fédéral en début d'année 2026, et que ses résultats seront dûment intégrés dans une stratégie nationale sur l'IA.

---

[75] Philippe Dufresne, Commissaire à la vie privée du Canada, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 2 février, 2025, https://www.ourcommons.ca/DocumentViewer/fr/45-1/ETHI/reunion-25/temoignages

[76] Article 33 de la LIAD, https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture