Mémoire sur le projet de loi C-27 : Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois

Présenté au Comité permanent des l'industrie et de la technologie de la Chambre des communes

Par la
Coalition pour la surveillance internationale des libertés civiles

22 septembre 2023

Coalition pour la surveillance internationale des libertés civiles
4, rue Florence, bureau 210, Ottawa (Ontario)
K2P 0W7
national.coordination@iclmg.ca |
https://iclmg.ca/fr/
613-241-5298

Introduction

La Coalition pour la surveillance internationale des libertés civiles (CSILC) est une coalition nationale de 45 organisations de la société civile canadienne fondée en 2002 à la suite de l'adoption de la première *Loi antiterroriste* du Canada. Au cours des deux décennies suivantes, nous avons travaillé de concert avec nos membres, les organismes partenaires, les communautés touchées et les législateurs afin de défendre les libertés civiles au Canada contre les excès et les abus au nom de la lutte antiterrorisme.

Dans le cadre de son travail, la coalition intervient couramment à l'égard des mesures législatives et des politiques gouvernementales qui suscitent des inquiétudes. Cela comprend la présentation de mémoires et la comparution devant des comités parlementaires, y compris dans le cadre des consultations fédérales sur la réforme de la *Loi sur la protection des renseignements* personnels[1], de la récente étude du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes sur les impacts de la technologie de reconnaissance faciale[2] et de l'étude du Comité permanent de la Chambre sur la cyber sécurité et la cyberguerre[3].

La protection de la vie privée, la lutte contre la surveillance et la défense des droits connexes sont au cœur de notre travail. À cet égard, nous avons mis sur pied la Campagne internationale contre la surveillance globale en 2005, nous avons réalisé des recherches sur la croissance exponentielle la surveillance gouvernementale et privée dans la foulée du 11 septembre et de la guerre au terrorisme et nous discutons avec les parlementaires sur des mesures législatives pour la protection des droits en matière de vie privée, notamment en nous opposant aux mesures qui porteraient atteinte à ces droits.

Dans l'esprit de ce travail, nous présentons des observations, ainsi que des propositions d'amendements concernant le projet de loi C-27, Loi de 2022 sur la mise en œuvre de la Charte du numérique. Notre mémoire porte sur les questions suivantes :

1. La Loi sur la protection de la vie privée des consommateurs (LPVPC)
    a. Reconnaissance de la vie privée en tant que droit de la personne
    b. Élimination des exemptions à l'égard du consentement pour des raisons de sécurité nationale
2. La Loi sur le Tribunal de la protection des renseignements personnels et des données (LTPRPD)
3. La Loi sur l'intelligence artificielle et les données (LIAD)
    a. Préoccupations globales
    b. Élargissement de la portée de la LIAD
    c. Modification de la définition de préjudice afin d'inclure les préjudices collectifs
    d. Annulation de l'exclusion de la technologie liée à la sécurité nationale

---

[1] CSILC, *Modernizing Canada's Privacy Act Consultation*, 15 février 2021. https://iclmg.ca/wp-content/uploads/2021/10/Privacy-Act-consultation-submission-ICLMG.pdf

[2] CSILC, Mémoire à propos de l'étude par le Comité de l'utilisation et des impacts de la technologie de reconnaissance faciale, 13 avril 2022. https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11789542/br-external/InternationalCivilLibertiesMonitoringGroup-106140660-f.pdf

[3] CSILC, *Submission to the Standing Committee on National Defence for its study on Cybersecurity and Cyberwarfare*, 6 avril 2023. https://iclmg.ca/wp-content/uploads/2023/04/NDDN-submission-re-cybersecurity-and-cyberwarfare.pdf

e. Disposition pour une surveillance et un examen indépendants

Notre expertise ne portant pas particulièrement sur la protection de la vie privée des consommateurs, nous ne formulerons pas de commentaires sur certaines parties de ce projet de loi. Nous soulignons toutefois que notre silence sur certains articles ne signifie pas que nous les approuvons, sachant que le projet de loi comporte plusieurs autres aspects à l'égard desquels des organismes de défense de la vie privée, des droits des consommateurs, des droits de la personne et des libertés civiles soulèvent des préoccupations. Nous espérons que notre contribution à votre étude de C-27 apportera un complément à la discussion générale.

1. La Loi sur la protection de la vie privée des consommateurs (LPVPC)

a. Reconnaissance de la vie privée en tant que droit de la personne

Il est fondamental que le Canada reconnaisse officiellement le droit à la vie privée en tant que droit de la personne. Il est louable que le préambule du projet de loi C-27 reconnaisse que le droit à la vie privée des individus est essentiel « à leur autonomie et à leur dignité et à la pleine jouissance des droits et libertés fondamentaux au Canada ». Cependant, l'inclusion de cet énoncé dans le préambule est insuffisante, parce que le préambule ne fait plus partie de la loi une fois le projet de loi adopté.

De nombreux précédents de reconnaissance explicite de la vie privée en tant que droit de la personne existent en droit canadien et en droit international.

D'abord, des décisions de la Cour suprême du Canada ont reconnu que les droits en matière de vie privée ont un statut quasi constitutionnel au Canada[4]. Le Commissariat à la protection de la vie privée du Canada a aussi énoncé clairement que le « droit de vivre et de s'épanouir à l'abri de la surveillance est un droit fondamental » et que « les citoyens peuvent circuler dans les espaces publics, semi-publics et privés sans risquer que leurs activités ne soient systématiquement recensées, suivies et surveillées[5] ».

Outre cette reconnaissance dans la loi et la jurisprudence canadiennes, le droit à la vie privée est également reconnu dans des accords internationaux, y compris des ententes fondamentales desquelles le Canada est un signataire de longue date.

Aux termes de l'article 17 du Pacte international relatif aux droits civils et politiques :

> 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

[4] *Lavigne c. Canada (Commissariat aux langues officielles)*, [2002] 2 RCS 773, par. 24.
[5] Commissariat à la protection de la vie privée du Canada, *Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, 2021, par 11. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/surveillance/police-et-securite-publique/gd_rf_202205/

> 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes[6].

Selon l'interprétation du Comité des droits de l'homme de l'ONU, ces dispositions exigent non seulement la protection contre la surveillance de l'État, mais aussi contre celle de toute personne morale ou physique[7].

Comme le souligne la spécialiste des questions de vie privée Teresa Scassa :

> La liberté d'association, les limites aux pratiques de surveillance abusives et la prévention de la discrimination fondée des données personnelles délicates ne sont que quelques exemples des effets sociaux de la protection du droit à la vie privée et des renseignements personnels. Les valeurs comme la démocratie et le pluralisme sont strictement liées à la protection de ces droits (p. 245). En matière de vie privée, une approche fondée sur les droits reconnaît non seulement le droit à la vie privée, mais aussi l'interrelation entre la vie privée et le droit des particuliers à exercer leurs autres droits et libertés en toute autonomie et dignité. En outre, le droit de la personne à la vie privée doit être fondé sur des lois qui le rendent effectif et applicable[8].

La nature fondamentale des droits en matière de vie privée ayant été reconnue par des tribunaux, des agents du Parlement et des organismes créés en vertu de traités internationaux, son absence du projet de loi C-27 constitue une importante lacune. La vie privée en tant que droit fondamental de la personne doit être explicitement comprise dans la loi afin qu'elle ait le poids juridique qu'elle mérite. Cela est particulièrement important dans le cas du projet de loi C-27, qui réglemente la protection de la vie privée des consommateurs et les activités du secteur privé.

En omettant de reconnaître la vie privée en tant que droit de la personne dans le projet de loi C-27, ce sont les intérêts des sociétés privées par rapport aux intérêts des particuliers qui sont mis en balance pour déterminer ce qui convient en matière de collecte, de conservation et d'utilisation des renseignements personnels. Le résultat est que les intérêts économiques l'emporteront probablement sur les intérêts de confidentialité des particuliers parce qu'ils ne seront pas soutenus en droit par le poids de la reconnaissance de la vie privée en tant que droit de la personne[9].

---

[6] Pacte international relatif aux droits civils et politiques, 16 décembre 1966, résolution de l'Assemblée générale 2200A (XXI). https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[7] Scassa, Teresa (2020), *A Human Rights-Based Approach to Data Protection in Canada*. [S.l.] : SSRN. https://ssrn.com/abstract=3620450.

[8] *Ibid* [TRADUCTION].

[9] OpenMedia, *Mémoire présenté au comité INDU pour son étude du projet de loi C-27, Loi de 2022 sur la mise en œuvre de la Charte du numérique*, 3 mai 2023. https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12448086/br-external/OpenMedia-10766527-f.pdf

<u>Recommandation 1:</u> Reconnaître la vie privée en tant que droit fondamental dans le texte du projet de loi C-27

<u>Amendement proposé</u> :
5 La présente loi a pour objet de fixer, dans une ère où les données circulent constamment au-delà des frontières et des limites géographiques et une part importante de l'activité économique repose sur l'analyse, la circulation et l'échange de renseignements personnels, des règles régissant la protection des renseignements personnels d'une manière qui tient compte, à la fois, du droit fondamental à la vie privée des individus…

b. Élimination des exemptions à l'égard du consentement pour des raisons de sécurité nationale

Nous sommes profondément inquiets que le projet de loi C-27 maintienne, en matière de consentement, des exemptions excessivement générales pour ce qui est de la collecte, de la conservation, de l'utilisation et de la communication des renseignements personnels pour des raisons de sécurité nationale.

Cela concerne notamment l'article 47, qui autorise une organisation du gouvernement à demander à des entités privées de communiquer des renseignements personnels dès lors qu'elle « soupçonne qu'ils concernent la sécurité nationale, la défense du Canada ou la conduite des affaires internationales », ainsi que l'article 48, qui autorise une entité privée à collecter, utiliser et communiquer des renseignements personnels à des organismes du gouvernement « si elle soupçonne que les renseignements concernent la sécurité nationale, la défense du Canada ou la conduite des affaires internationales ».

Premièrement, de telles dispositions sont en contradiction avec l'objet du projet de loi C-27 énoncé à l'article 5, ainsi qu'avec les « fins acceptables » prévues au paragraphe 12(1).

Aux termes de l'article 5, le projet de loi établit des règles d'une manière qui protège à la fois le droit à la vie privée des individus et le besoin des organisations « de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Aux termes du paragraphe 12(1), « […] l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins et d'une manière qu'une personne raisonnable estimerait acceptables dans les circonstances. »

Bien que les articles 30 (Situation d'urgence : utilisation), 43 (Application du droit : demande de l'institution gouvernementale) et 44 (Contrôle d'application : demande de l'institution gouvernementale) autorisent la communication de renseignements personnels sans consentement, ils présentent des justifications valables : intervention en cas d'urgence, application d'une loi fédérale ou provinciale, ou tenue d'une enquête pour l'application d'une loi fédérale ou étrangère. Les ministères doivent mentionner la source de l'autorité légitime étayant leur droit d'obtenir les renseignements, et les exceptions se limitent à la communication.

Même l'article 45, qui établit une exception plus générale permettant aux entités privées de communiquer de leur propre initiative des renseignements personnels concernant une contravention à une loi, exige que l'entité privée ait des **motifs raisonnables de croire** « que les renseignements concernent une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être ».

On pourrait soutenir que chacun de ces articles respecte le critère des motifs raisonnables, compte tenu des circonstances particulières, et qu'ils prévoient des protections appropriées (quoique minimales).

Cependant, l'article 47(1) autorise la communication de renseignements personnels sans consentement à la demande d'un organisme gouvernemental au seul motif que l'organisme « **soupçonne** qu'ils concernent la sécurité nationale, la défense du Canada ou la conduite des affaires internationales ». Ce critère est beaucoup moins rigoureux que ce qui est prévu aux articles 30, 43 ou 44.

En outre, les paragraphes 47(2) et (3) autorisent aussi une entité privée à collecter et utiliser des renseignements personnels sans consentement aux fins du paragraphe 47(1), ce qui va également beaucoup plus loin que ce que prévoient d'autres dispositions semblables. Cela va manifestement au-delà de ce que l'on pourrait considérer comme une utilisation « raisonnable » ou « acceptable » des renseignements personnels. De plus, rien ne justifie qu'une exemption plus large soit accordée sur de simples soupçons concernant « la sécurité nationale, la défense du Canada ou la conduite des affaires internationales ». Laisser l'article 47 dans le projet de loi créerait un régime où l'on permet aux organismes gouvernementaux d'obtenir en secret des renseignements auprès d'entités privées en s'appuyant sur des motifs mal définis fondés sur la simple présomption que les renseignements « concernent la sécurité nationale, la défense du Canada ou la conduite des affaires internationales ». Cela suscite non seulement de graves préoccupations en matière de vie privée, mais aussi des préoccupations relatives à d'éventuels abus d'un pouvoir de collecte de renseignements et de surveillance de particuliers ou de communautés en fonction d'une simple présomption que les renseignements « concernent la sécurité nationale, la défense du Canada ou la conduite des affaires internationales », plutôt qu'en fonction de motifs de croire que les renseignements concernent une contravention au droit fédéral ou provincial.

L'article 48 suscite des préoccupations encore plus importantes : le paragraphe 48(1) autorise l'entité privée à communiquer sans consentement, de sa propre initiative, des renseignements personnels à des organismes gouvernementaux, encore une fois pour des raisons concernant « la sécurité nationale, la défense du Canada ou la conduite des affaires internationales ». Or, contrairement à l'article 45, en ce qui concerne la communication de renseignements liés à une contravention à une loi fédérale, l'entité privée doit seulement **soupçonner** que les renseignements communiqués concernent la sécurité nationale – ce qui est beaucoup moins exigeant que le critère des « motifs raisonnables de croire » prévu à l'article 45.

À l'instar de l'article 47, l'article 48 comporte les paragraphes (2) et (3), lesquels autorisent l'entité privée à collecter et utiliser des renseignements personnels aux fins du paragraphe 48(1). Le résultat est que l'entité privée serait en mesure de collecter, d'utiliser et de communiquer des renseignements personnels sans consentement en se fondant uniquement sur la présomption qu'ils concernent la sécurité nationale, la défense ou les affaires internationales. Le domaine de

la sécurité nationale étant extraordinairement vaste par définition et le motif de la sécurité nationale ayant été maintes fois utilisé pour justifier la surveillance et l'incrimination abusives et illégales de diverses communautés au Canada, il est impossible de voir en quoi cela peut être considéré comme une fin raisonnable et acceptable. En fait, on peut raisonnablement prévoir que cela entraînerait la collecte excessive de renseignements personnels et leur communication abusive à des organismes gouvernementaux, donnant lieu à des violations non seulement des droits en matière de vie privée, mais aussi du droit à la liberté d'expression, du droit à la liberté de réunion et du droit à l'égalité.

Recommandation 2 : Que l'article 47 soit supprimé de la LPVPC, ou qu'il soit modifié afin de respecter le critère des motifs raisonnables de croire et qu'il soit limité à la communication.

Amendement proposé a) :
Supprimer intégralement les paragraphes 47(1) à (3)

OU, amendement proposé b) :
47 (1) L'organisation peut communiquer les renseignements personnels d'un individu, à son insu ou sans son consentement, à l'institution gouvernementale — ou à la subdivision d'une telle institution — qui les a demandés en mentionnant la source de l'autorité légitime étayant son droit de les obtenir et le fait qu'elle a des motifs raisonnables de croire ~~soupçonne~~ qu'ils concernent une menace imminente à la sécurité nationale, la défense du Canada ou la conduite des affaires internationales.

~~(2) L'organisation peut recueillir les renseignements personnels d'un individu, à son insu ou sans son consentement, en vue de la communication visée au paragraphe (1).~~

~~(3) L'organisation peut utiliser les renseignements personnels d'un individu, à son insu ou sans son consentement, s'ils ont été recueillis au titre du paragraphe (2).~~

Recommandation 3 : Que l'article 48 soit supprimé du projet de loi C-27, ou qu'il respecte le critère des motifs raisonnables de croire et qu'il soit limité à la communication.

Amendement proposé a) :
Supprimer intégralement les paragraphes 48(1) à (3)

OU, amendement proposé b) :
48 (1) L'organisation peut, de sa propre initiative, communiquer les renseignements personnels d'un individu, à son insu ou sans son consentement, à une institution gouvernementale ou une subdivision d'une telle institution si elle a des motifs raisonnables de croire ~~soupçonne~~ qu'ils concernent une menace imminente à la sécurité nationale, la défense du Canada ou la conduite des affaires internationales.

~~(2) L'organisation peut recueillir les renseignements personnels d'un individu, à son insu ou sans son consentement, en vue de la communication visée au paragraphe (1).~~

~~(3) L'organisation peut utiliser les renseignements personnels d'un individu, à son insu ou sans son consentement, s'ils ont été recueillis au titre du paragraphe (2).~~

2. La Loi sur le Tribunal de la protection des renseignements personnels et des données

Pour que soient dûment respectées les lois du Canada sur la protection de la vie privée dans le secteur privé, il est essentiel que l'organisme chargé de la surveillance des mesures de protection de la vie privée ait les pouvoirs nécessaires pour le faire. Nous accueillons donc favorablement l'établissement dans la LPVPC de nouveaux pouvoirs permettant au Commissariat à la protection de la vie privée du Canada de prendre des ordonnances afin d'obliger les entités privées à :

- prendre des mesures pour se conformer à la LPVPC;
- cesser d'agir en contravention de la LPVPC;
- respecter un accord de conformité;
- prendre publique toute action prise ou envisagée pour corriger les politiques, les pratiques ou les procédures que l'entité a mises en place afin de respecter les obligations qui lui incombent sous le régime de la LPVPC.

De plus, la LPVPC autoriserait le Commissariat à imposer des sanctions administratives pécuniaires (SAP) aux entités fautives.

Ce sont là des améliorations importantes et nécessaires aux pouvoirs du Commissariat pour assurer la protection des droits en matière de vie privée au Canada et le respect de la réglementation sur la vie privée.

Nous craignons toutefois que le Tribunal de la protection des renseignements personnels et des

données que l'on propose d'instituer à la partie deux du projet de loi C-27 ne fera qu'affaiblir ces nouveaux pouvoirs[10]. Comme d'autres l'on fait, nous observons que la capacité du tribunal à approuver les SAP et à trancher les appels concernant les ordonnances et les sanctions diminue non seulement les pouvoirs du Commissariat, mais aussi l'indépendance du processus. Le Commissariat à la protection de la vie privée est un agent du Parlement complètement indépendant, nommé en consultation avec les autres partis. Les membres du tribunal, quant à eux, sont nommés par le gouverneur en conseil, sur la recommandation du ministre concerné, ce qui pourrait faire en sorte que les ordonnances rendues par un agent indépendant soient annulées en appel par un organisme moins indépendant.

En outre, comme le souligne le Commissariat : « Les provinces qui ont des lois sur la protection des renseignements personnels dans le secteur privé essentiellement similaires ne disposent pas de ce type de tribunal administratif agissant comme organe de contrôle[11]. » Les recherches d'OpenMedia montrent aussi que des États comparables comme le Royaume-Uni, l'Union européenne, la Nouvelle-Zélande et l'Australie ont également renoncé à un tribunal d'examen du travail des responsables de la protection de la vie privée[12].

Recommandation 4 : Que la Loi sur le Tribunal de la protection des renseignements personnels et des données soit supprimée du projet de loi C-27 et remplacée par un processus où les ordonnances peuvent être portées en appel directement à la Cour fédérale du Canada.

Amendement proposé :
Supprimer la *Partie 2 – Loi sur le Tribunal de la protection des renseignements personnels et des données* du projet de loi C-27.

3. La Loi sur l'intelligence artificielle et les données

a. Préoccupations globales

Dans le cadre de notre travail, nous constatons les importantes répercussions négatives que peut avoir sur les moyens d'existence et sur les droits de la population au Canada et à l'étranger l'absence de réglementation sur les outils d'intelligence artificielle et la façon dont ils sont utilisés. Cela comprend l'utilisation de l'intelligence artificielle pour alimenter les outils de surveillance, pour catégoriser les individus, pour tenter de prédire des activités illégales ou pour prendre des décisions pouvant avoir des conséquences décisives sur la vie des personnes concernées dans nombre de domaines névralgiques, notamment l'emploi, l'immigration, la sécurité aux frontières, l'application de la loi et la collecte du renseignement.

Nous sommes particulièrement conscients de l'intérêt que portent les organismes

[10] OpenMedia 2023
[11] Commissariat à la protection de la vie privée du Canada, *Mémoire du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-27, la Loi de 2022 sur la mise en œuvre de la Charte du numérique*, avril 2023. https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12370320/br-external/OfficeOfThePrivacyCommissionerOfCanada-brief-f.pdf
[12] OpenMedia 2023

gouvernementaux, les organismes d'application de la loi et les organismes du renseignement à l'exploitation des outils d'IA et à la collaboration avec les entreprises privées qui travaillent sur ces outils, pour les besoins de la lutte contre le terrorisme et de la sécurité nationale. Nous avons aussi vu comment de tels outils peuvent être utilisés pour violer les droits fondamentaux et comment divers acteurs peuvent obtenir, acheter, fournir ou voler de tels outils à leurs propres fins malhonnêtes.

Au vu de ce qui précède, nous sommes profondément conscients de l'importance de réglementer le développement et l'utilisation des outils d'IA dans le secteur privé. Or, après l'avoir évaluée, nous croyons que la Loi sur l'intelligence artificielle et les données (LIAD) proposée n'est pas adéquate pour atteindre cet objectif.

À cet égard, nous maintenons les réserves suivantes sur la LIAD, comme nous les avons déjà formulées dans une lettre au gouvernement et aux chefs de parti[13] :

- De nombreux aspects de la loi seront déterminés par règlement, après l'adoption du projet de loi, un processus moins transparent soumis à un examen moins minutieux.
- Le mécanisme de surveillance proposé est arbitraire et le mécanisme d'exécution est fragile, en raison notamment du manque d'indépendance du poste de commissaire à l'intelligence artificielle et aux données que l'on propose de créer.
- La loi ne s'applique pas aux institutions gouvernementales ni aux organismes chargés de la sécurité nationale. Cela ouvre la porte à des abus potentiels, comme l'utilisation illégale de la technologie de reconnaissance faciale de Clearview AI par la Gendarmerie royale du Canada (GRC).
- La loi ne tient pas compte des implications substantielles des systèmes algorithmiques pour les droits de la personne.
- Dans le cadre de l'examen plus vaste du projet de loi C-27, la LIAD ne fera pas l'objet d'un examen aussi minutieux que requis.
- Le comité ne peut pas mener le genre de consultations publiques nécessaires pour tenir compte des lacunes du projet de loi, consultations que le gouvernement aurait dû tenir avant de déposer le projet de loi.
- Les amendements clés nécessaires pour corriger les lacunes du projet de loi iraient au-delà de ce que le comité pourrait faire, par exemple faire appliquer la loi aux institutions gouvernementales ou établir un organisme de supervision adéquat et indépendant.

Pour toutes ces raisons, nous recommandons que le comité supprime la LIAD du projet de loi C-27 afin que la question de la réglementation de l'intelligence artificielle au Canada soit soumise à un processus de consultation publique plus rigoureux et transparent et qu'un projet de loi renforcé soit présenté au Parlement une fois élaboré.

[13] Lettre exhortant les chefs de parti à voter contre la LIAD en deuxième lecture, 14 mars 2023. https://iclmg.ca/vote-against-aida/ [EN ANGLAIS SEULEMENT]

Recommandation 5 : Que le comité supprime la LIAD du projet de loi C-27 afin que la question de la réglementation de l'intelligence artificielle au Canada soit soumise à un processus de consultation publique plus rigoureux et transparent et qu'un projet de loi renforcé soit présenté au Parlement une fois élaboré.

Cependant, nous sommes aussi conscients que, à cette étape, la LIAD pourrait très bien être adoptée. Si nous ne croyons pas que la loi puisse être suffisamment modifiée pour véritablement corriger les problèmes fondamentaux qu'elle comporte, nous formulons les suggestions suivantes afin de régler certains problèmes essentiels.

b. Élargissement de la portée de la LIAD

À l'heure actuelle, le cadre réglementaire proposé par la LIAD ne s'appliquerait qu'aux « systèmes à incidence élevée ». À l'avenant d'un problème généralisé dans la LIAD, le terme « système à incidence élevée » n'est pas défini dans la loi, sa définition étant plutôt laissée au processus réglementaire. Cela suscite plusieurs inquiétudes graves :

Premièrement, sans une définition claire du terme « système à incidence élevée », il est impossible de déterminer les technologies qui seraient visées par la loi. Dans ces circonstances, le public et les parlementaires qui étudient le projet de loi ne peuvent avoir l'assurance que le régime proposé sera adéquat et efficace.

Deuxièmement, en confiant la définition au seul processus réglementaire, le processus de définition du terme « système à incidence élevée » échappe à la transparence et à la rigueur de l'étude du Parlement. Les règlements sont souvent adoptés sans être soumis au même examen rigoureux que les projets de loi, de sorte qu'un processus qui souffrait déjà d'un manque de transparence et d'un déficit consultatif pourrait devenir encore plus opaque.

Troisièmement, si le processus réglementaire offre de la souplesse, le fait de s'en remettre à un tel processus pour établir une définition qui sous-tend tout le cadre de la LIAD pourrait entraîner l'affaiblissement ultérieur du cadre réglementaire.

En outre, le fait de restreindre la LIAD à la réglementation des « systèmes à incidence élevée » constitue en problème en soi. S'il est évident que les « systèmes à incidence élevée » doivent être réglementés, la loi ne dit rien sur les systèmes d'IA présentant d'autres niveaux de préjudice. Cela signifierait que les nombreux types de systèmes d'IA, qui comportent des impacts très divers, devraient être bien classés dans deux catégories. Cette restriction posera probablement des problèmes substantiels à l'avenir, comme ceux qui surviendront sans doute rapidement avec les systèmes d'IA générative. De surcroît, cette approche est déphasée par rapport à ce qui se fait ailleurs, comme dans l'UE. Par exemple, le projet de loi sur l'IA de l'UE propose d'établir quatre catégories précises pour les systèmes d'IA, chacune assortie d'un niveau de réglementation progressif :

- Risque inacceptable
- Risque élevé
- IA générative
- Risque limité

Les systèmes d'IA à « risque inacceptable » seraient des systèmes qui posent un risque tellement important pour les droits qu'ils doivent être interdits; les systèmes d'IA à « risque élevé » nécessiteraient un travail d'analyse et d'évaluation considérable avant de pouvoir être utilisés; les systèmes d'IA à « risque limité » auraient à respecter des exigences en matière de transparence et de consentement des utilisateurs[14].

Nous recommandons que le comité modifie la LIAD afin d'y introduire des catégories progressives pour les systèmes d'IA à réglementer, en s'inspirant des définitions prévues dans la loi sur l'IA de l'UE. Nous recommandons aussi que de nouvelles catégories puissent au besoin être ajoutées par règlement, afin de pouvoir adapter le cadre réglementaire en fonction des besoins, tout en assurant un niveau de réglementation minimal.

Enfin, la LIAD omet aussi d'indiquer comment un système d'IA est classé dans la catégorie des systèmes « à incidence élevée ». Au terme de l'article 7, une telle évaluation peut simplement être faite par le « responsable d'un système d'intelligence artificielle ». Pour évaluer le niveau d'incidence d'un système d'IA, il est essentiel que des critères clairs et indépendants soient établis. Nous appuyons la recommandation faite par le FAEJ dans son mémoire sur la LIAD, à savoir qu'une évaluation doit comporter un audit en matière d'équité et de vie privée selon ce que prévoit la réglementation, ainsi que d'autres amendements connexes, que nous présentons ci-dessous[15].

Recommandation 6 : Que la LIAD soit modifiée de manière à y inclure des catégories de systèmes d'IA autres que les « systèmes à incidence élevée », d'y définir de façon non exhaustive les niveaux de risque associés à chaque catégorie et à veiller à ce que le classement soit fondé sur un audit en matière d'équité et de vie privée. (NOTA : les amendements b) et c) s'inspire principalement des propositions du mémoire du FAEJ, p. 11 et 13)

Amendement proposé a) :
5 (1) Les définitions qui suivent s'appliquent à la présente partie.
…
Système inacceptable s'entend de… [insérer la définition]
Système à incidence élevée s'entend de… [insérer la définition]
Système à faible incidence s'entend de… [insérer la définition]

Amendement proposé b) :
- Supprimer l'article 7 et supprimer « incidence élevée » des articles 8, 9, 11 et 12.

Amendement proposé c) :
8 Le responsable d'un système ~~à incidence élevée~~ d'IA établit, conformément aux règlements,

[14] Parlement européen, *Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle*. https://www.europarl.europa.eu/news/fr/headlines/society/20230601STO93804/loi-sur-l-ia-de-l-ue-premiere-reglementation-de-l-intelligence-artificielle

[15] Kim, Rosel et Thomasen, Kristen, Mémoire au Comité permanent de l'industrie et de la technologie au sujet du projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, 11 septembre 2023, p. 11 et 13. https://ssrn.com/abstract=4571389 [FAEJ 2023] [EN ANGLAIS SEULEMENT]

des mesures visant à cerner, évaluer et atténuer les risques de préjudice ou de résultats biaisés que pourrait entraîner la création ou l'utilisation du système d'intelligence artificielle. Cela doit comprendre l'exécution d'un audit en matière d'équité et de vie privée selon ce qui est prévu par règlement.

11 (1) La personne qui rend disponible un système ~~à incidence élevée~~ d'IA publie, sur un site Web accessible au public, selon toute modalité fixée par règlement, une description, en langage clair, du système qui prévoit, notamment, les éléments suivants :

a) l'utilisation visée;
b) le contenu qu'il est censé générer, les prédictions ou recommandations qu'il est censé faire ou les décisions qu'il est censé prendre;
c) les résultats d'un audit en matière d'équité et de vie privée selon ce qui est prévu par règlement;…

36 Le gouverneur en conseil peut prendre des règlements concernant l'application de la présente partie, notamment des règlements :
b) établissant les critères pour ~~l'application de~~ la définition ou l'ajout de catégories de systèmes d'IA ~~système à incidence élevée~~ au paragraphe 5(1);
(x1) établissant les critères pour la surveillance et la gestion des systèmes d'IA par les personnes responsables;
(x2) énonçant les exigences relatives aux audits des systèmes d'IA en matière d'équité et de vie privée.

c. Modification de la définition de préjudice afin d'inclure les préjudices collectifs

Dans la version actuelle de la LIAD, la définition du terme préjudice se limite à un préjudice physique ou psychologique subi par un individu, aux dommages à ses biens ou aux pertes économiques qu'il subit. Cette définition ne tient aucun compte de l'existence avérée des préjudices collectifs que cause l'IA en portant atteinte aux droits collectifs. Comme l'explique le FAEJ :

« Les droits collectifs sont les droits qu'a un groupe dans son ensemble, contrairement aux droits individuels, qui sont ceux que possèdent les membres du groupe individuellement. Les droits collectifs protègent les intérêts du groupe, comme les droits culturels et linguistiques, le droit collectif à la vie privée, les droits environnementaux, ainsi que les droits des travailleurs et les droits syndicaux, qui sont tous grandement menacés par l'avènement des systèmes d'IA[16] ».

Les outils d'intelligence artificielle peuvent porter atteinte aux droits collectifs de nombreuses façons. Sur le plan de la sécurité nationale, ces préjudices comprennent la sélection ou la catégorisation de personnes en fonction du risque évalué pour des fins d'immigration, d'emploi, de voyage ou même de surveillance. Ils comprennent aussi le recours aux systèmes d'intelligence artificielle pour mener des activités de surveillance et d'enquête à l'égard de groupes entiers en fonction de critères programmée dans les outils d'IA, ainsi que les préjudices subis par des groupes entiers vivant avec les conséquences de systèmes biaisés qui n'arrivent pas à bien reconnaître les personnes de certaines races, de certains âges ou certains genres. Ces outils peuvent aussi être utilisés pour définir (et exclure) des catégories de personnes pour l'obtention de services financiers. Outre la sécurité nationale, les préjudices collectifs peuvent également prendre la forme d'autres violations des droits de la personne, de violations des droits en matière d'emploi ou de violations des droits de propriété intellectuelle, entre autres[17].

Nous appuyons de nouveau la recommandation du FAEJ sur cette question, à savoir que l'article 5 devrait être modifié afin de tenir compte des préjudices collectifs[18].

---

[16] FAEJ 2023, p. 6 [TRADUCTION].

[17] Voir Blair Attard-Frost, *Les systèmes d'IA générative : Répercussions sur les artistes et les créateurs et lacunes associées de la Loi sur l'intelligence artificielle et les données*, mémoire soumis au Comité permanent de l'industrie et de la technologie, 5 juin 2023, p. 14. https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12541028/br-external/AttardFrostBlair-10776569-f.pdf; FAEJ 2023; Bailey, J., Burkell, J. et McPhail, B. *Submissions on Bill C-27: The Digital Charter Implementation Act*, septembre 2023.

[18] FAEJ 2023, p. 5

Recommandation 7 : Modifier l'article 5 afin d'élargir la définition de préjudice en y ajoutant les préjudices collectifs.

Amendement :
5 (1) ***préjudice*** Préjudice physique ou psychologique subi par un individu ou un groupe identifiable, dommage à ses biens, à des biens en propriété collective, à des biens immeubles détenus au nom d'un groupe, à des biens collectifs ou publics ou à des espaces publics, ou perte économique subie par un individu ou un groupe identifiable.

d. Annulation de l'exclusion de la technologie liée à la sécurité nationale

À l'échelle internationale, l'intérêt à l'égard de l'utilisation des outils d'intelligence artificielle pour la sécurité nationale et la lutte contre le terrorisme connaît une augmentation phénoménale. On les utilise pour surveiller le contenu terroriste en ligne, mener des activités de surveillance, analyser des données pour reconnaître des tendances et prévoir des activités terroristes, guider des armes télécommandées et autonomes et rendre des décisions ou catégoriser des personnes ou des groupes en fonction du risque en matière d'immigration, d'emploi ou de voyage.

Chacun de ces usages comporte certains des risques les plus graves pour les droits de la personne, dont la liberté d'expression, la liberté d'association, la liberté de circulation, le droit à la sécurité personnelle, le droit à l'égalité, le droit à la vie privée et d'autres encore.

Les organismes de sécurité nationale du Canada comme la GRC, l'ASFC, le SCRS et le CST ont ouvertement manifesté leur intérêt pour les outils d'intelligence artificielle et parlé de l'utilisation qu'ils en font à de nombreuses fins, y compris la reconnaissance faciale, la surveillance, la sécurité des frontières, l'analyse de données et la cybersécurité. Ils n'ont toutefois pas révélé comment ils utilisent les systèmes d'intelligence artificielle exactement, ni les mesures qu'ils prennent pour éviter les préjudices. En outre, aucun cadre précis n'existe afin de réglementer leur utilisation de ces outils afin de prévenir des préjudices graves à des particuliers ou des groupes.

La LIAD offre l'occasion de combler cette lacune, en réglementant l'utilisation que font les organismes de sécurité nationale de la technologie du secteur privé. Il est donc stupéfiant de constater qu'au paragraphe 3(2), la LIAD fait le contraire en mentionnant expressément que la loi ne s'applique pas aux :

> […] produits, services ou activités qui relèvent de la compétence ou de l'autorité des personnes suivantes :
>
> a) le ministre de la Défense nationale;
> b) le directeur du Service canadien du renseignement de sécurité;
> c) le chef du Centre de la sécurité des télécommunications;
> d) toute autre personne qui est responsable d'un ministère ou

d'un organisme fédéral ou provincial et qui est désignée par règlement.

Cela signifierait que tout système d'IA créé par un acteur du secteur privé relavant de la compétence ou de l'autorité du gouvernement ne serait soumis à aucune réglementation ou supervision indépendante. Une telle exclusion est totalement inacceptable.

Comme l'a dit la Rapporteuse spéciale sur les droits de l'homme et la lutte antiterroriste de l'ONU au Comité des droits de l'homme de l'ONU en mars 2023, « la Rapporteuse spéciale est profondément inquiète de la pratique bien établie des États d'adopter des lois qui exemptent de l'application des régimes de supervision réguliers l'utilisation de l'IA à des fins militaires et de sécurité nationale[19] ».

Toujours selon le rapport :

« La Rapporteuse met en évidence l'utilisation des impératifs de sécurité et de la lutte contre le terrorisme pour justifier la création, l'utilisation et le transfert de technologies nouvelles, y compris, les technologies biométriques, l'IA, les véhicules aériens sans pilote (drones) et les outils de surveillance. Elle critique la façon dont, sous prétexte de prévenir le terrorisme, on utilise des technologies nouvelles qui, en pratique, compromettent gravement les droits des personnes et des communautés. Des technologies à risque élevé sont introduites discrètement en invoquant des motifs de sécurité, alors qu'en fait elles affaiblissent la sécurité collective et nuisent à la promotion et à la protection des droits de la personne[20] ».

En présentant l'exemple de la loi sur l'IA de l'UE, la Rapporteuse souligne que « les systèmes d'IA créés à des fins militaires ou mixtes devraient être réglementés par la loi sur l'IA. Elle soutient que la conception, la création et l'utilisation des systèmes d'IA destinés à la défense nationale doivent relever de la convention du Conseil de l'Europe. Autrement, il en résulterait que le projet de convention ne tiendrait aucun compte des préoccupations qui, en matière de droits de la personne, revêtent un grand intérêt dans la région[21]. »

Des inquiétudes semblables s'appliquent à la LIAD en ce qui concerne l'exclusion des systèmes d'IA conçus pour les organismes de sécurité nationale du Canada. Tous les systèmes d'IA conçus par le secteur privé doivent être réglementés, peu importe qu'ils soient utilisés par des organismes de sécurité nationale. Si le gouvernement soutient que si cette technologie est vendue sur le marché privé, elle sera alors réglementée, il fait fi des graves répercussions que pourrait avoir, et qu'aura certainement l'usage d'une technologie non réglementée par ces organismes. Il fait également fi de la possibilité que cette technologie puisse être piratée ou transmise illégalement, ou qu'elle puisse être créée à l'intention d'un organisme canadien puis vendue dans des marchés sans réglementation rigoureuse en matière d'IA. De plus, nous

---

[19] *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, Rapport de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Fionnuala Ní Aoláin. Conseil des droits de l'homme, cinquante-deuxième session, A/HRC/52/39, 1er mars 2023. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx [TRADUCTION].

[20] *Ibid*.
[21] *Ibid*.

craindrions que la conception non réglementée pour usage gouvernemental ne donne lieu à des pressions pour l'assouplissement de la réglementation sur une éventuelle reformulation de la technologie pour le secteur privé.

Recommandation 8 : Supprimer le paragraphe 3(2) de la LIAD

Amendement proposé :
~~Produits, services ou activités~~
~~(2) Elle ne s'applique pas non plus à l'égard des produits, services ou activités qui relèvent de la compétence ou de l'autorité des personnes suivantes :~~
~~a) le ministre de la Défense nationale;~~
~~b) le directeur du Service canadien du renseignement de sécurité;~~
~~c) le chef du Centre de la sécurité des télécommunications;~~
~~d) toute autre personne qui est responsable d'un ministère ou d'un organisme fédéral ou provincial et qui est désignée par règlement.~~

e. Disposition pour une surveillance et un examen indépendants

Dans sa forme actuelle, le projet de loi confie l'application de la LIAD et l'élaboration de la réglementation connexe au ministre de l'Innovation, des Sciences et du Développement économique, qui peut déléguer tous ses pouvoirs (sauf celui de prendre des règlements) à un cadre supérieur du Ministère à titre de commissaire à l'intelligence artificielle et aux données.

Cette disposition devrait être révisée en sorte que soit constitué un agent du Parlement indépendant, de l'extérieur d'ISDE, afin de superviser l'application de la réglementation sur l'IA. Il est inopportun que ce poste relève d'ISDE, dont le mandat englobe la promotion de l'industrie de l'IA. Il arrivera inévitablement que les besoins réglementaires entreront en conflit avec les intérêts de l'industrie de l'IA; lorsque cela se produira, il sera essentiel d'avoir un organisme de réglementation indépendant qui ne soit pas exposé à ce conflit d'intérêts potentiel (ou même à l'apparence d'un tel conflit).

Nous recommandons donc que la LIAD soit modifiée afin de prévoir la création d'un organisme de réglementation indépendant :

- Le commissaire à l'IA et aux données est nommé par le gouverneur en conseil après consultation des chefs des partis d'opposition à la Chambre des communes et approbation de la nomination par résolution du Sénat et de la Chambre des communes.
- Le commissaire est chargé de l'exécution et du contrôle d'application de la présente partie.
- Le commissaire a le titre d'administrateur général.
- Le commissaire a le pouvoir de nommer et de congédier des employés, d'exiger les attestations de sécurité voulues, etc.

Le reste de la LIAD serait ensuite modifié afin de remplacer, dans les dispositions concernées, le mot « ministre » par « commissaire à l'IA et aux données ».

Il serait également possible de modifier le paragraphe 33(2) afin de simplement autoriser la

constitution d'un agent indépendant, mais cela ne garantirait pas qu'un organisme de réglementation indépendant serait créé et qu'il ne relèverait pas d'ISDE.

<u>Recommandation 9</u> : Que la LIAD soit modifiée afin de créer un poste de commissaire à l'intelligence artificielle et aux données chargé superviser l'exécution et le contrôle d'application de la loi.

<u>Proposition a)</u> :

- Modifier l'article 32 pour indiquer ceci :
    - Le commissaire à l'IA et aux données est nommé par le gouverneur en conseil après consultation des chefs des partis d'opposition à la Chambre des communes et approbation de la nomination par résolution du Sénat et de la Chambre des communes.
    - Le commissaire est chargé de l'exécution et du contrôle d'application de la présente partie.
    - Le commissaire a le titre d'administrateur général.
    - Le commissaire a le pouvoir de nommer et de congédier des employés, d'exiger les attestations de sécurité voulues, etc.

(suite)

- Modifier le reste de la LIAD, y compris les articles 13 à 21, pour faire dépendre du commissaire les pouvoirs d'exécution et de contrôle d'application.

Proposition b)

- Modifier le paragraphe 33(2) afin d'autoriser la création d'un organisme de réglementation indépendant.
- Modifier le reste de la LIAD, y compris les articles 13 à 21, pour faire dépendre de l'organisme de réglementation indépendant les pouvoirs d'exécution et de contrôle.

Il sera aussi essentiel d'évaluer au fil du temps l'efficacité et l'effet des dispositions de la LIAD. La LIAD devra aussi être réévaluée et faire l'objet de modifications pour tenir compte de l'évolution que connaîtra assurément le domaine de l'IA, malgré les tentatives de « pérennisation ». Pour ce faire, la loi devrait comporter des dispositions pour qu'elle fasse l'objet d'un rapport annuel et d'un examen périodique.

Recommandation 10 : Que la LIAD soit modifiée afin d'exiger que la loi fasse l'objet d'un rapport annuel public et d'un examen quinquennal.

Amendements proposés :

Rapports

38 Dans les trois mois suivant la fin de chaque exercice, le commissaire à l'intelligence artificielle et aux données (le commissaire), présente au Parlement le rapport des activités du commissariat au cours de l'exercice.

39 Le commissaire peut, à toute époque de l'année, présenter au Parlement un rapport spécial sur toute question relevant de ses pouvoirs et fonctions et dont l'urgence ou l'importance sont telles, selon lui, qu'il serait contre-indiqué d'en différer le compte rendu jusqu'à l'époque du rapport annuel suivant.

40 (1) La présentation des rapports du commissaire au Parlement s'effectue par remise au président du Sénat et à celui de la Chambre des communes pour dépôt devant leurs chambres respectives.

(2) Les rapports visés au paragraphe (1) sont, après leur dépôt, renvoyés devant le comité désigné ou constitué par le Parlement en application du paragraphe 75(1).

(suite)

41 (1) Dans les trois mois suivant la fin de chaque exercice, le commissaire présente au ministre le rapport confidentiel des activités du Commissariat ne pouvant être divulguées publiquement.

(2) Dans les trente jours suivant la présentation du rapport au ministre, un résumé du rapport est déposé au Parlement.

42 (1) Le commissaire peut, à toute époque de l'année, présenter au ministre un rapport spécial confidentiel sur toute question relevant de ses pouvoirs et fonctions et dont l'urgence ou l'importance sont telles, selon lui, qu'il serait contre-indiqué d'en différer le compte rendu jusqu'à l'époque du rapport annuel suivant.

(2) Dans les trente jours suivant la présentation du rapport au ministre, un résumé du rapport est déposé au Parlement.

43 Tout rapport confidentiel sur des questions de sécurité nationale est également transmis au Comité des parlementaires sur la sécurité nationale et le renseignement et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.

Examen

44 (1) Tous les cinq ans à compter de la date d'entrée en vigueur de la présente loi, le comité, soit de la Chambre des communes, soit du Sénat, soit mixte, désigné ou constitué à cette fin procède à l'examen de l'application de la présente loi.

(2) Dans les 90 jours suivant la réception du rapport du comité, le ministre fait déposer devant chaque chambre du Parlement un rapport en réponse à l'examen du comité.

(3) Si le rapport du comité relève des lacunes dans l'application de la présente loi, le ministre présente dans son rapport un plan pour les corriger — comprenant toute proposition de modification législative — ainsi qu'un échéancier pour sa mise en œuvre.

**Renuméroter les articles subséquents de la loi*