— Un rapport du Centre juridique —

5 mai 2026

Le danger de l'intelligence artificielle contrôlée par le gouvernement

Comment l'IA contrôlée par l'État menace notre vie privée, notre autonomie et la liberté d'expression – et comment le projet de loi C-22 ouvre la voie

Auteur : Nigel Hannaford

Centre juridique
pour les libertés constitutionnelles

Nous défendons
la liberté d'un océan
à l'autre.

Résumé

Ce rapport examine l'état actuel des politiques publiques au Canada en ce qui concerne l'intelligence artificielle (IA), y compris les appels récents à réglementer ou même nationaliser l'IA. De telles propositions interviennent à la suite de la fusillade de masse de Tumbler Ridge en février 2026 et de l'échec perçu d'OpenAI (propriétaire de ChatGPT) à divulguer à la police les interactions du tireur avec ChatGPT. Bien qu'elles soient présentées comme nécessaires à la sécurité publique, ces propositions risquent de placer les interactions privées des Canadiens avec l'IA sous surveillance et contrôle de l'État. Ce rapport soutient que de telles mesures – en plus de l'ambition du projet de loi C-22 d'élargir l'accès de l'État aux données personnelles – menacent les droits protégés par la Charte à la vie privée, à la liberté d'expression et à l'autonomie en normalisant l'accès gouvernemental à des renseignements personnels sensibles sans supervision judiciaire adéquate. Il conclut que la sécurité publique doit être assurée par des garanties bien adaptées et visant à protéger les libertés fondamentales des Canadiens.

Droits d'auteur et réimpression

Centre juridique
pour les libertés constitutionnelles

Remerciements

Nous remercions les milliers de Canadiens qui continuent de soutenir le Centre juridique pour les libertés constitutionnelles (CJLC) grâce à leurs dons. Leur générosité donne au CJLC le pouvoir de défendre la liberté au Canada et de façonner les politiques publiques qui respectent les droits et libertés de la Charte.

Mises à jour de ce rapport

Ceci est la version 1.1 de ce rapport, qui peut être mise à jour périodiquement.

À propos de l'auteur

Ce rapport a été rédigé par le journaliste chevronné et analyste en politiques publiques Nigel Hannaford.

Avertissement : Ce rapport traite de ChatGPT, un produit d'OpenAI. C'est une publication indépendante et elle n'est ni affiliée ni approuvée par OpenAI.

Table des matières

Résumé exécutif

La fusillade de masse de février à Tumbler Ridge, en Colombie-Britannique, a été la fusillade de masse la plus meurtrière au Canada depuis 1989. En juin 2025, huit mois avant l'attaque, OpenAI (la société d'IA propriétaire de ChatGPT) a suspendu le compte ChatGPT du tireur Jesse Van Rootselaar après que des examens internes ont signalé des discussions décrivant des scénarios de violence armée. Les employés d'OpenAI ont toutefois déterminé que le contenu ne respectait pas son seuil de « danger imminent » ou de « risque crédible de préjudice physique grave » et n'ont donc pas signalé les discussions à la police. Ce n'est qu'après la fusillade qu'OpenAI a révélé les discussions.

Le discours public et gouvernemental est rapidement passé du contrôle des armes à feu à l'échec perçu d'OpenAI et à la responsabilité des entreprises privées d'intelligence artificielle (IA) en général. Le gouvernement fédéral a laissé entendre qu'il pourrait introduire de nouvelles lois concernant les entreprises privées d'IA. Les analystes politiques ont appelé à une IA nationalisée – ou contrôlée par le gouvernement –, soutenant que seuls les systèmes contrôlés par le gouvernement peuvent assurer la responsabilité, la surveillance démocratique et la sécurité publique.

Le contrôle gouvernemental (nationalisation ou réglementation) des entreprises privées d'IA aurait un coût très élevé : il pourrait facilement faciliter la surveillance étatique de routine des conversations privées. La surveillance d'État menace la vie privée, érode la liberté d'expression et introduit un biais politique dans la modération du contenu. Parmi ses nombreuses utilisations, l'IA est un outil d'exploration privée – tester des idées, rédiger des arguments et explorer les doutes. La nationalisation et la réglementation donneraient au gouvernement fédéral un large pouvoir pour influencer l'utilisation de l'IA par les Canadiens, un peu comme le *Conseil de la radiodiffusion et des télécommunications canadiennes* (CRTC) influence de manière inappropriée le contenu que les Canadiens découvrent à travers la radiodiffusion et la diffusion en continu. De plus, de telles réponses à Tumbler Ridge pourraient violer le droit des Canadiens à la protection contre les fouilles et saisies déraisonnables.

Le projet de loi C-22, la *Loi sur l'accès légal* (présentée au Parlement en mars 2026), abaisse déjà le seuil permettant aux forces de l'ordre d'accéder à ce que les Canadiens disent et font en ligne. Le projet de loi abaisse le seuil légal d'accès aux informations des abonnés, passant de « motifs raisonnables de croire » à « motifs raisonnables de soupçonner » – facilitant ainsi l'obtention d'informations sensibles des abonnés par la police. En vertu de ce projet de loi, le gouvernement fédéral peut également exiger que les « fournisseurs de services électroniques » conservent les métadonnées (définition en note de bas[1] de page) et créent une capacité intégrée pour une divulgation possible aux forces

[1] Les métadonnées (ou « données sur les données ») sont des informations qui, lorsqu'elles sont agrégées, peuvent révéler les schémas détaillés de comportement, d'associations et d'intérêts personnels d'un individu. Cela inclut les informations sur les abonnés telles que le nom, l'adresse physique, les informations

de l'ordre. Les critiques soulignent la conservation obligatoire des métadonnées comme l'un des outils les plus intrusifs en matière de vie privée disponibles, créant des capacités de surveillance dérobée dépassant les objectifs anti-criminalité déclarés.[2] Compte tenu de la définition extrêmement large du projet de loi C-22[3] des « fournisseurs de services électroniques »,[4] des plateformes d'IA comme OpenAI seront probablement aussi incluses dans cette législation, ouvrant la voie à un degré sans précédent de surveillance étatique.

Bien que la sécurité publique soit un objectif légitime, elle doit être atteinte sans étendre l'accès de l'État aux interactions avec l'IA, ce qui normaliserait la surveillance, éroderait l'anonymat, refroidirait l'exploration intellectuelle et mènerait à une autocensure persistante. Une société où les citoyens doivent réfléchir à deux fois avant de poser une question n'est pas une société libre.

Les gouvernements doivent poursuivre leurs objectifs légitimes tout en respectant les droits et libertés garantis par la Charte des Canadiens, y compris le droit à la vie privée et à la liberté contre la surveillance étatique. Le Centre juridique pour les libertés constitutionnelles (CJLC) conclut que le Parlement devrait :

- Résister aux appels à nationaliser ou contrôler de manière centralisée les systèmes d'IA
- Rejeter le projet de loi C-22 et ses dispositions sur la conservation des métadonnées et l'accès forcé
- Maintenir des exigences rigoureuses en matière de mandat pour tous les accès étatiques aux données personnelles, limitant cet accès aux circonstances impliquant des menaces graves, imminentes et crédibles

---

de facturation, ainsi que le moment où vous avez ouvert le compte, quand et où vous accédez au service, l'emplacement et les mouvements physiques, avec qui vous avez communiqué, l'heure et la durée des appels, ainsi que les adresses IP utilisées, etc. (Voir ce site Web du gouvernement du Canada avec une liste détaillée des données incluses dans les métadonnées : https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/)

[2] Michael Geist, entre autres.

[3] Le projet de loi C-22 définit le terme « fournisseur de services électroniques » de façon si large qu'il englobe essentiellement tous les services sur Internet et plus encore : « fournisseur de services électroniques désigne une personne qui, individuellement ou au sein d'un groupe, fournit un service électronique, y compris dans le but de permettre les communications, et qui (a) fournit le service à des personnes au Canada; ou (b) exerce tout ou partie de ses activités commerciales au Canada. »

[4] Le projet de loi C-22 vise généralement les fournisseurs de services électroniques ou de télécommunications, pas seulement les fournisseurs de services Internet. Cette portée plus large est délibérée et reflète le droit moderne des communications, où de nombreuses entités – pas seulement les FAI – détiennent les données et métadonnées des abonnés pertinentes aux régimes d'accès légal.

Grâce à ces mesures, le Canada peut répondre à des préoccupations légitimes en matière de sécurité sans sacrifier les libertés fondamentales qui sous-tendent une société libre et démocratique.

Introduction

En février 2026, ChatGPT d'OpenAI (chef de file de l'IA) attirait environ 900 millions d'utilisateurs par semaine pour le travail, les études et des besoins personnels.[5] Partout dans le monde, les gens utilisent la technologie pour des tâches aussi complexes que le développement logiciel, l'ingénierie et la modélisation financière, pour des sujets aussi banals que la planification d'un jardin ou d'un programme de mise en forme, et même pour des aspects aussi personnels que le counseling. De plus en plus, l'IA est l'ingénieur, l'analyste de données, le moteur de recherche, le résolveur de problèmes et, dans certains cas, la confident.

Ce rapport répond aux appels à la surveillance gouvernementale de l'IA qui ont émergé à la suite de la fusillade de l'école de Tumbler Ridge en Colombie-Britannique en février 2026. OpenAI est le point central de la réaction du public. Certains réclament la nationalisation de l'IA, ou une législation qui obligerait les entreprises privées d'IA à signaler aux forces de l'ordre des conversations concernant l'IA. Ce rapport aborde les implications constitutionnelles tant d'un modèle d'IA public que de la réglementation des entreprises privées d'IA.

Bien que la nationalisation et la réglementation soient formulées en termes de sécurité publique, de sûreté et de souveraineté, elles normaliseraient l'accès gouvernemental routinier aux communications privées sans autorisation judiciaire. Le progrès technologique ne devrait pas exiger de renoncer à des libertés fondamentales.

Ce rapport examine également le projet de loi C-22, la *Loi sur l'accès légal*. S'il est adoptée, ce projet de loi transformerait probablement OpenAI (et d'autres entreprises d'IA) en « fournisseurs de services électroniques », compte tenu de sa définition large du terme, ce qui donnerait au gouvernement fédéral et aux forces de l'ordre des pouvoirs beaucoup plus grands pour accéder aux informations des utilisateurs.

Tumbler Ridge, OpenAI et la réaction du public

Le 10 février 2026, Jesse Van Rootselaar de Tumbler Ridge, en Colombie-Britannique, a abattu sa mère et son demi-frère cadet dans leur maison. Puis, à l'école secondaire voisine, Van Rootselaar a assassiné six élèves et membres du personnel scolaire. Van Rootselaar a blessé 27 autres avant de mourir d'une blessure auto-infligée. Il s'agissait de la fusillade scolaire la plus meurtrière au Canada depuis 1989.

[5] Malik, Aisha. « ChatGPT atteint 900 millions d'utilisateurs actifs hebdomadaires » TechCrunch. 27 février 2026. https://techcrunch.com/2026/02/27/chatgpt-reaches-900m-weekly-active-users/

La conversation nationale ne s'est pas longtemps attardée sur la question politique perpétuelle de la violence armée. Au lieu de cela, l'attention du public s'est tournée vers le manque de soutiens en santé mentale dans des communautés éloignées comme Tumbler Ridge, mais aussi sur le rôle qu'OpenAI a joué – ou, comme certains le diraient, « échoué » à jouer – dans la fusillade.

Huit mois plus tôt, en juin 2025, OpenAI avait suspendu le compte ChatGPT de Van Rootselaar après qu'il eut été signalé en interne pour des discussions décrivant des scénarios de violence armée. Après que plusieurs employés d'OpenAI eurent analysé les choses à l'interne, OpenAI a déterminé que Van Rootselaar devait être banni de la plateforme pour « mauvaise utilisation de [ses] modèles en vue d'activités violentes ».[6] Cependant, OpenAI n'a pas informé les forces de l'ordre, après avoir déterminé que le contenu des discussions ne constituait ni un danger imminent ni un risque crédible de préjudice physique grave. Après la fusillade de masse, OpenAI a divulgué l'historique des discussions de Van Rootselaar à la police.

Nationaliser l'IA?

Le 1er mars 2026, Nathan E. Sanders et Bruce Shneier ont soutenu dans le *Globe and Mail* que « OpenAI a démontré qu'on ne peut pas lui faire confiance. Le Canada a besoin d'une IA publique et nationalisée »[7] en réponse au lien – aussi vague soit-il – d'OpenAI avec la fusillade de masse de Tumbler Ridge. Ils soutiennent que les plateformes d'IA privées sont guidées par des valeurs commerciales qui entrent en conflit avec la sécurité, la transparence et le bien public. Selon eux, les plateformes d'IA sont concentrées dans des juridictions étrangères et fonctionnent avec une transparence limitée et un contrôle démocratique.

Les auteurs y soutenaient également que l'IA fonctionne aujourd'hui comme une infrastructure publique critique – comme la radiodiffusion publique, les réseaux électriques et les autoroutes – et qu'il est temps que le gouvernement fédéral développe une IA nationalisée et contrôlée par le gouvernement. En pratique, cela pourrait signifier la création de modèles d'IA financés par le gouvernement, supervisés par des institutions publiques ou des agences fédérales. L'IA serait à la technologie de l'information ce que la *CBC* est à la radiodiffusion.

---

[6] L'hiver, Jesse. « Les messages ChatGPT du tireur de Tumbler Ridge ont été signalés des mois avant l'attaque. » Le Globe and Mail. 20 février 2026. Malik, Aisha. « ChatGPT atteint 900 millions d'utilisateurs actifs hebdomadaires » TechCrunch. 27 février 2026. https://techcrunch.com/2026/02/27/chatgpt-reaches-900m-weekly-active-users/?utm_source=chatgpt.com. Consulté le 22 avril 2026.

[7] Sanders, Nathan E. et Bruce Schneier. « OpenAI a montré qu'on ne peut pas lui faire confiance. Le Canada a besoin d'une IA publique et nationalisée. » Schneier sur la sécurité. 1er mars 2026. https://www.schneier.com/essays/archives/2026/03/openai-has-shown-it-cannot-be-trusted-canada-needs-nationalized-public-ai.html

Pour Sanders et Schneier, l'IA est trop puissante pour que son utilisation dans de larges pans de la société soit laissée à un marché libre. « En revanche, » ont-ils conclu, « l'IA publique développée par des agences transparentes et responsables permettrait aux processus démocratiques et à la supervision politique de régir le fonctionnement de ces puissants systèmes », ce qui est une hypothèse non fondée selon laquelle les gouvernements sont plus transparents et responsables que les entreprises privées.

Cette chronique du *Globe and* Mail n'est pas un simple vœu pieux. Dans un communiqué de presse de septembre 2025,[8] le gouvernement fédéral a annoncé le lancement d'un *groupe de travail sur la stratégie IA* et un « sprint national de 30 jours qui aidera à façonner l'approche du Canada envers l'IA » – une approche présentée non seulement comme une innovation technologique de routine, mais comme une étape vers la sécurisation de la « souveraineté numérique » au milieu de « profonds bouleversements géopolitiques ».[9]

L'ambition d'Ottawa n'est pas seulement de soutenir l'investissement dans le développement de technologies d'IA privées au Canada. Dans un communiqué de presse du 15 avril 2026, le gouvernement fédéral a annoncé un effort national pour « construire l'un des systèmes de supercalcul d'intelligence artificielle (IA) les plus avancés ».[10] Il est important de noter que cette infrastructure sera détenue par des Canadiens, c'est-à-dire par le gouvernement. Parallèlement, dans le cadre de sa *Stratégie souveraine de calcul en IA*, le gouvernement fédéral dépense 700 millions de dollars pour développer l'infrastructure et la capacité de calcul en IA pour les utilisateurs canadiens.

Ce que fait actuellement le gouvernement fédéral semble cocher toutes les cases pour Sanders et Schneier : un ou plusieurs modèles d'IA appartenant à l'État, développés et soutenus au Canada, et soumis aux lois et règlements canadiens.

Réglementation accrue de l'IA?

La famille de la jeune victime Maya Gebala de la fusillade de masse de Tumbler Ridge a intenté une poursuite devant la Cour suprême de la Colombie-Britannique contre OpenAI, alléguant qu'OpenAI a agi de manière négligente en ne signalant pas l'historique de discussion de Van Rootselaar aux forces de l'ordre. Dans leur *avis de réclamation civile*, la famille (les plaignants) a qualifié ChatGPT de « confident, collaborateur, allié et ami de confiance » et a allégué que Van Rootselaar « s'est appuyé sur ChatGPT pour la santé

[8] Gouvernement du Canada. Innovation, Sciences et Développement économique Canada. « Le gouvernement du Canada lance un groupe de travail sur la stratégie IA et l'engagement public pour le développement de la prochaine stratégie IA. » 26 septembre 2025. https://www.canada.ca/en/innovation-science-economic-development/news/2025/09/government-of-canada-launches-ai-strategy-task-force-and-public-engagement-on-the-development-of-the-next-ai-strategy.html.
[9] Ibid
[10] Ibid.

mentale et le counseling, le traitant comme un conseiller et/ou un pseudo-thérapeute en santé mentale. »[11]

Les plaignants soutiennent donc qu'OpenAI avait un « devoir de diligence de signaler des cas de risques de blessures corporelles graves ou de décès pour des personnes identifiées avec une spécificité raisonnable...[12] » La poursuite demande effectivement au tribunal d'élargir les obligations de diligence à une plateforme d'IA et présente même ChatGPT comme un participant actif ou un facilitateur de la fusillade de masse.

Peu après la fusillade de masse, le ministre fédéral de l'IA, Evan Solomon, a convoqué à Ottawa les principaux représentants de la sécurité d'OpenAI pour expliquer ses politiques d'escalade concernant les discussions d'IA signalées. « Ils viendront ici, et nous aurons une réunion pour expliquer leurs protocoles de sécurité, leur escalade et leurs seuils d'escalade auprès de la police, afin que nous comprenions mieux ce qui se passe et ce qu'ils font », a déclaré le ministre Solomon aux journalistes.[13]

Le ministre Solomon a exprimé sa déception face à cette rencontre. Les représentants de la sécurité d'OpenAI l'avaient informé que la politique de l'entreprise est de transmettre les conversations aux forces de l'ordre seulement lorsqu'elles indiquent « un risque imminent et crédible de dommages physiques graves à autrui. »[14]

En réponse à la négligence présumée d'OpenAI, le gouvernement fédéral a envisagé trois solutions : interdire ChatGPT au Canada,[15] forcer OpenAI à modifier ses politiques d'escalade (ce qu'OpenAI a depuis fait),[16] ou introduire une législation fédérale pour réglementer toutes les entreprises d'IA opérant au Canada (ce que le ministre Solomon et le ministre de la Justice Sean Fraser ont menacé de faire).[17]

---

[11] La famille de Van Rootselaar. Avis de réclamation civile. Cour suprême de la Colombie-Britannique. https://www.courthousenews.com/wp-content/uploads/2026/03/tumbler-ridge-openAI.pdf, à la page 8.
[12] Ibid.
[13] Cecco, Leyland. « Le Canada cherche des réponses auprès d'OpenAI pour ne pas avoir alerté la police après avoir suspendu le compte du tireur dans une école. » The Guardian. 23 février 2026. https://www.theguardian.com/world/2026/feb/23/openai-tumber-ridge-shooter-account-suspended
[14] Singh, Divyadeep. « La société mère de ChatGPT, OpenAI, a banni le compte du tireur scolaire de Tumbler Ridge, en Colombie-Britannique, a envisagé d'alerter la police canadienne, mais a retenu pour cette raison. » The Economic Times. 21 février 2026. https://economictimes.indiatimes.com/news/international/canada/chatgpts-parent-company-openai-banned-tumbler-ridge-b-c-school-shooters-account-mulled-alerting-canadian-police-but-held-back-over-this-reason/articleshow/128636101.cms
[15] Woolf, Marie. 25 février 2026. « Ottawa avertit d'une législation si OpenAI n'apporte pas de changements après que l'historique des discussions ait déclenché des signaux d'alarme. » Le Globe and Mail. 25 février 2026. https://www.theglobeandmail.com/politics/article-openai-justice-minister-legislation-tumbler-ridge-shooter-chat-history/
[16] Hunter, Justine et Joe Castaldo. « OpenAI affirme que les récents changements de politique auraient signalé les messages du tireur de Tumbler Ridge à la police. » Le Globe and Mail. 26 février 2026. https://www.theglobeandmail.com/canada/article-openai-chatgpt-tumbler-ridge-shooter-reporting-policies-changes/. Consulté le 10 avril 2026.
[17] Tumilty, Ryan. « Le ministre canadien de l'IA annonce qu'OpenAI va changer ChatGPT après la fusillade de Tumbler Ridge. » The Star. 6 mars 2026. https://www.thestar.com/politics/federal/canada-s-ai-minister-

Plus tard, le 4 mars 2026, le ministre Solomon a informé le PDG d'OpenAI, Sam Altman, que « des experts canadiens devront évaluer les conversations sur ChatGPT qui ont été signalées comme présentant des indices qu'un utilisateur a l'intention de causer un préjudice imminent, afin de déterminer s'il convient d'alerter les forces de l'ordre »[18] Le premier ministre de la Colombie-Britannique, David Eby, a demandé au gouvernement fédéral de légiférer un seuil minimum de signalement « afin de s'assurer que la protection de la communauté, la protection des enfants passe avant les intérêts des actionnaires »[19] – un argument similaire à celui proposé par Sanders et Schneier.

La nationalisation et la réglementation vont toutes deux dans la même direction : intégrer l'utilisation de l'IA par les Canadiens dans le domaine de la surveillance et/ou du contrôle du gouvernement fédéral.

La nationalisation ou la réglementation de l'IA sont-elles vraiment efficaces?

Les événements survenus à Tumbler Ridge soulèvent la question de savoir si les mesures législatives de nationalisation ou de régulation de l'IA auraient été efficaces pour prévenir cette tragédie dès le départ. Huit mois entiers ont séparé l'attaque de l'utilisation de ChatGPT par Van Rootselaar. Simultanément, Van Rootselaar avait déjà eu des contacts avec les forces de l'ordre, qui avaient retiré des armes à feu de la maison en 2024, mais les avaient retournées moins d'un mois avant la fusillade.[20] Un secteur de l'IA contrôlé par l'État ou fortement réglementé aurait-il pu faire une différence dans ce cas?

De plus, en supposant – comme le font Sanders et Schneier dans l' article du *Globe and Mail* – que placer l'IA sous contrôle gouvernemental assurerait une plus grande transparence et reddition de comptes, c'est supposer que les gouvernements sont intrinsèquement plus transparents, plus responsables et plus compétents à gérer l'IA que les entreprises privées. Bien que nous ne suggérions pas que les entreprises privées ont toujours les mains propres, cette hypothèse n'est pas évidente et est contredite par des développements législatifs fédéraux récents tels que C-2, C-8 et C-22. Ces projets de loi élargiraient les pouvoirs gouvernementaux pour exiger l'accès aux données des utilisateurs, tout en leur permettant de garder ces demandes secrètes vis-à-vis des utilisateurs concernés.

---

says-openai-to-change-chatgpt-after-tumbler-ridge-shooting/article_0c5daccf-e6dd-4bfd-b657-6e154a5caf23.html. Consulté le 10 avril 2026.

[18] Castaldo, Joe. « Le ministre de l'IA dit à OpenAI que les experts canadiens doivent évaluer les conversations ChatGPT signalées. » Le Globe and Mail. 4 mars 2026. https://www.theglobeandmail.com/business/article-ai-minister-tells-altman-canadian-experts-must-assess-flagged-chatgpt/ Consulté le 10 avril 2026.

[19] Ibid.

[20] Pruden, Jana G, Matthew Scace et Alanna Smith. « Unis dans le deuil : une communauté soudée de Tumbler Ridge se serre les coudes face à une tragédie 'inimaginable'. » Publié le 13 février 2026. Consulté le 28 avril 2026. https://www.theglobeandmail.com/canada/article-tumbler-ridge-community-tragedy-school-shooting/

La nationalisation ou la réglementation stricte de l'IA entraînerait plusieurs conséquences négatives sérieuses pour les droits et libertés des Canadiens.

Implications constitutionnelles de la nationalisation et de la réglementation de l'IA

Les Canadiens se soucient profondément de la préservation de la sécurité publique et du bon ordre, surtout à la suite d'une fusillade de masse. Si des réponses législatives ou politiques à Tumbler Ridge doivent être poursuivies, de telles mesures doivent respecter les droits et libertés garantis par la *Charte* des Canadiens. Mais un secteur de l'IA public ou fortement réglementé accomplirait le contraire.

1. Biais gouvernemental et « influence »

Si l'histoire et les précédents sont un indice, une plateforme d'IA nationalisée ou fortement réglementée est susceptible d'être soumise aux biais et aux ambitions du gouvernement qui la contrôle.

Par exemple, dans sa réglementation de l'industrie de la radiodiffusion privée, le gouvernement fédéral exige que les diffuseurs et les services de diffusion en ligne diffusent des niveaux obligatoires de contenu dit « canadien ». Ce qui constitue un contenu « canadien » est toutefois déterminé par le gouvernement fédéral. Avec l'adoption de la *Loi sur la diffusion en ligne*[21] en 2023, tous les services de diffusion en continu (par exemple, Netflix, YouTube et Spotify) relèvent désormais de l'autorité réglementaire du CRTC, ce qui lui permet d'influencer les algorithmes et la « découverte » du contenu, peu importe les goûts des consommateurs, ce qui influence ce que les consommateurs sont plus susceptibles de voir.

De plus, grâce à la *Loi sur les nouvelles en ligne* de 2023, [22] Meta n'autorise plus les Canadiens à publier des liens vers des articles d'actualité sur Facebook et Instagram – perturbant ainsi l'accès de millions de Canadiens à l'information sur le monde. Malgré la pression publique et même les menaces internationales de représailles,[23] le gouvernement fédéral n'a ni abrogé ni modifié la législation.

Ces pouvoirs d'interférer avec l'expérience en ligne des Canadiens ne se limiteront peut-être pas longtemps au contenu diffusé ou aux nouvelles en ligne.

---

[21] Parlement du Canada. *Projet de loi C-11 : Loi sur la diffusion en ligne en ligne*. 44e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-11

[22] Parlement du Canada. *Projet de loi C-18 : Loi sur les nouvelles en ligne.* 44e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-18

[23] Boynton, Sean. « Un projet de loi républicain vise la Loi sur la diffusion en ligne et menace de représailles. » Global News. Publié le 19 mars 2025. Consulté le 10 avril 2026. https://globalnews.ca/news/11738344/cusma-online-streaming-act-us-bill-tariffs/

Un gouvernement fédéral contrôlant un modèle d'IA nationalisé aura le pouvoir de programmer la manière dont ce modèle est utilisé par les chercheurs, les innovateurs et les Canadiens ordinaires. Et c'est précisément le genre de programmabilité que Sanders et Schneier demandent : si les entreprises privées d'IA ne peuvent pas être dignes de confiance pour signaler les discussions alarmantes des utilisateurs aux forces de l'ordre, alors il suffit de développer une plateforme d'IA contrôlée par l'État qui ne peut pas « s'endormir à son poste ». Mais l'influence ou le contrôle gouvernemental à des fins néfastes n'est impensable. Il y a seulement quatre ans, l'activité parfaitement légale de faire un don à une manifestation pacifique faisait l'objet d'une surveillance financière et a entraîné le gel des comptes bancaires, démontrant que le gouvernement n'est pas toujours une force pour le bien.

Que l'ingérence de l'État provienne d'un modèle d'IA appartenant à l'État ou d'une réglementation accrue des entreprises d'IA privées, l'État pourrait intervenir ou « guider » les interactions avec l'IA des utilisateurs précisément parce que ces interactions se produiraient dans le cadre de l'autorité de l'État, aussi privées que soient ces interactions pour les utilisateurs.

2. Érosion de la vie privée

Lorsque l'État possède et contrôle les plateformes d'IA, la frontière entre l'usage privé et la surveillance de l'État disparaît. Les Canadiens connaissent déjà des environnements où leur comportement semble privé mais ne l'est pas.

Les employés comprennent que les employeurs ont le droit (ainsi que la capacité technique) de surveiller toute activité survenant sur le matériel et les logiciels fournis par l'entreprise, peu importe à quel point ces communications peuvent sembler privées pour l'employé. Les citoyens qui apprécient les bibliothèques publiques comprennent que ces institutions publiques tiennent souvent des registres de chaque livre, magazine et film emprunté et pourraient donc théoriquement servir à profiler les usagers. De la même façon, les Canadiens utilisant un modèle d'IA appartenant à l'État comprendraient que l'État aurait à la fois le droit et la capacité technique – même si elle n'est pas exercée – de surveiller et d'imposer des contraintes à toutes les utilisations du modèle d'IA. La question de savoir si les utilisateurs jouissent de la vie privée dépendrait entièrement du choix volontaire du gouvernement de s'abstenir de voir quels Canadiens accèdent à l'IA, ainsi que le contenu de ces interactions. C'est une protection fragile.

La réglementation des entreprises privées d'IA suscite la même préoccupation en matière de vie privée, mais dans une moindre mesure. Les entreprises privées d'IA réglementées par le gouvernement seraient à un degré de distance de l'État. Cependant, l'État pourrait toujours dicter aux entreprises d'IA ce qui compte comme des « requête des utilisateurs à examiner par les forces de l'ordre » et ordonner à ces entreprises réglementées de remettre les communications privées aux forces de l'ordre. Par excès de prudence, pour éviter d'être accusés de non-respect, les entreprises d'IA réglementées peuvent choisir de remettre aux forces de l'ordre toute requêt qui éveille le moindre soupçon. Il serait rationnel pour toute entreprise d'IA opérant au Canada d'adopter cette approche du «

mieux vaut prévenir que guérir », avec pour conséquence malheureuse et prévisible que des informations privées non criminelles soient divulguées aux forces de l'ordre. Dans ce scénario, les entreprises d'IA divulgueraient de manière proactive aux forces de l'ordre les informations des utilisateurs *avant* l'intervention policière et *en dehors* du processus traditionnel de mandat. Essentiellement, les entreprises d'IA deviendraient des intermédiaires dans un programme croissant de surveillance étatique.

Les tribunaux canadiens et la protection de la vie privée

L'article 8 de la *Charte canadienne des droits et libertés* protège les Canadiens contre les fouilles et saisies déraisonnables.[24] Cette protection constitutionnelle sous-tend l'autonomie personnelle, la dignité, la vie privée, le contrôle de nos renseignements personnels et la protection contre la surveillance étatique.

La Cour suprême du Canada a à plusieurs reprises confirmé que l'article 8 de la *Charte* protège un droit large et significatif à la vie privée à l'ère numérique. Dans l'*affaire R c. Spencer (2014),*[25] la Cour a statué que la vie privée inclut le droit de contrôler la diffusion des renseignements personnels et a souligné que l'anonymat est un élément central de cette protection. La Cour a en outre reconnu que les individus conservent une attente raisonnable de vie privée dans leurs communications électroniques, même lorsque ces communications sont stockées ou transmises par des systèmes tiers (*R c. Marakah 2017*;[26] *R c. Reeves 2018*). [27]

Plus important encore, la Cour a averti que l'État ne peut pas contourner les protections constitutionnelles en s'appuyant sur des intermédiaires pour obtenir des informations auxquelles il ne pourrait pas légalement accéder directement (*R c. Duarte, 1990*). [28]

Appliqués à l'IA, ces principes ont des implications importantes. Les interactions avec l'IA révèlent souvent le « noyau biographique » de l'information personnelle : les pensées, les questions et les idées en développement des utilisateurs. Lorsque ces interactions sont directement surveillées par l'État, ou lorsque les entreprises privées sont effectivement contraintes de les divulguer, cela sape les protections mêmes que *l'article 8 de la Charte* vise à garantir. Que la vie privée soit violée par l'État ou par des entreprises privées qui remettent des données à l'État, le résultat est le même : l'accès à des informations profondément personnelles sans supervision judiciaire significative, contraire à l'exigence constitutionnelle selon laquelle l'intrusion de l'État doit être soigneusement limitée, autorisée et justifiée.

Restreindre l'autonomie : pensée, exploration intellectuelle et expression

---

[24] Gouvernement du Canada. *La Charte canadienne des droits et libertés.* Centre juridique pour les libertés constitutionnelles. https://www.jccf.ca/the-canadian-charter-of-rights-and-freedoms/
[25] R. c. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212. Paragraphe 49
[26] R. c. Marakah, 2017 SCC 59, [2017] 2 S.C.R. 608. Para. 10
[27] R. c. Reeves, 2018 SCC 56, [2018] 3 S.C.R. 531. Para. 17-22
[28] R. c. Duarte, [1990] 1 R.C.S. 30.

Les limites imposées à la protection garantie par l'article 8 de la *Charte* contre les fouilles, perquisitions et saisies abusives compromettent la capacité des Canadiens à exercer pleinement leur liberté d'expression, leur autonomie personnelle et leur droit d'être à l'abri des ingérences injustifiées de l'État — un objectif fondamental de la *Charte*.

La liberté d'expression dépend d'une liberté antérieure – la liberté d'explorer des idées en privé avant de les présenter publiquement. Les écrivains, chercheurs, étudiants et citoyens ordinaires doivent pouvoir expérimenter avec des idées inconnues ou troublantes sans craindre que leurs pensées préliminaires soient consignées, analysées ou jugées. Si les utilisateurs d'IA en viennent à croire que leurs interactions sont surveillées, l'autocensure devient un comportement rationnel et répandu. Les individus éviteront les questions spéculatives, les sujets controversés ou les scénarios imaginatifs qui pourraient être interprétés à tort comme des intentions criminelles. L'innovation ralentit lorsque les gens hésitent à tester des pistes non conventionnelles. Le débat démocratique s'affaiblit lorsque les citoyens s'abstiennent de développer des arguments en privé avant de les exprimer en public.

En effet, les utilisateurs d'IA abordent souvent des sujets difficiles ou même troublants pour un large éventail de fins : recherche académique, écriture créative,[29] analyse professionnelle ou réflexion personnelle. Un cadre réglementaire qui encourage ou exige le signalement des entrées « préoccupantes » des utilisateurs risque de faire s'effondrer ces distinctions. En pratique, la réglementation gouvernementale de l'IA peut considérer l'activité exploratoire ou expressive comme suspecte, particulièrement lorsque le contexte est incomplet ou mal compris. Le résultat n'est pas seulement le risque de surdéclaration, mais aussi l'érosion d'un espace où les individus peuvent penser, questionner et créer sans craindre d'interprétations erronées. Le problème tient à l'incapacité des systèmes d'IA – et de ceux qui les régulent – à distinguer de manière fiable l'intention nuisible de l'exploration légitime. Et, en ce qui concerne le droit à la vie privée des citoyens, *la fiabilité est importante*.

Atteinte à la vie privée et autocensure – Une étude de cas

Après qu'on eut découvert en 2013 que la National Security Agency (NSA) menait des opérations de surveillance de masse sur des millions de téléphones, de comptes courriel, de forums de discussion et des comportements et transactions en ligne américains, de nombreux auteurs ont signalé s'autocensurer afin d'éviter la surveillance de l'État. Selon une enquête menée en 2013 auprès d'écrivains américains par Pen America et le FDR Group,[30] 85 % des participants (tous écrivains) ont déclaré s'inquiéter de la surveillance gouvernementale. Soixante-six pour cent ont déclaré désapprouver que le gouvernement

[29] Selon un sondage de l'Authors Guild auprès de romanciers professionnels, 67% des écrivains utilisent des outils d'écriture par IA.

[30] Le groupe FDR. « Effets dissuasifs : la surveillance de la NSA pousse les écrivains américains à s'autocensurer. » PEN America. 12 novembre 2013. https://pen.org/report/chilling-effects/

collecte des données Internet et télécommunications dans le cadre de leur guerre contre le terrorisme.[31]

Le sondage a révélé que 16 % des écrivains évitaient d'écrire ou de parler de certains sujets afin d'éviter des répercussions négatives.[32] Cette réticence expressive était particulièrement marquée chez les auteurs et chercheurs enclins à critiquer le gouvernement ou à aborder des sujets sensibles, notamment la politique étrangère, la sécurité nationale et les critiques du gouvernement.

Une telle autocensure reflète le risque inhérent à l'élargissement de la surveillance étatique des interactions avec l'IA.

Le projet de loi C-22 et l'IA

Le projet de loi C-22, la *Loi sur l'accès légal*,[33] est la plus récente tentative du gouvernement fédéral en matière de législation sur l'« accès légal » – une ambition de longue date des gouvernements fédéraux, à commencer par le projet de loi C-74, la *Loi sur la modernisation des techniques d'enquête*,[34] en 2005. S'il est adopté, le projet de loi pourrait introduire la surveillance étatique de l'IA en abaissant le seuil permettant aux forces de l'ordre d'accéder aux données des utilisateurs.

Le projet de loi C-22 a été présenté le 12 mars 2026, succédant à la très critiquée *Loi sur les frontières* fortes (projet de loi C-2), qui introduisait de larges pouvoirs de surveillance et des dispositions d'accès sans mandat. Présenté comme une législation « protégeant les Canadiens », le projet de loi C-22 est (au moment de la rédaction) devant le Comité permanent de la sécurité publique et de la sécurité nationale.

Le projet de loi C-22 élargit l'accès de la police et du renseignement aux données numériques des Canadiens, y compris les interactions des utilisateurs avec l'IA. Il exige que les « fournisseurs de services électroniques » aident la police et le renseignement à acquérir ces données. Le projet de loi définit le « service électronique » de façon très large comme impliquant la « création, l'enregistrement, le stockage, le traitement, la transmission, la réception, l'émission ou la mise à disposition d'informations sous forme électronique, numérique ou toute autre forme immatérielle…[35] » Cela couvre pratiquement toutes les communications entre personnes et entre personnes et systèmes numériques en permanence, à l'exception des lettres papier, journaux, dépliants, affiches

---

[31] Ibid.
[32] Ibid.
[33] Parlement du Canada. *Projet de loi C-22 : Loi relative à l'accès légal*. 45e Parlement, 1re session. Première lecture. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-22.
[34] Parlement du Canada. Projet de loi C-74 : Loi sur la modernisation des techniques d'enquête. 38e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/DocumentViewer/en/38-1/bill/C-74/first-reading
[35] Parlement du Canada. *Projet de loi C-22 : Loi relative à l'accès légal*. 45e Parlement, 1re session. Première lecture. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-22. Deuxième partie, 2(1).

et panneaux publicitaires. Le projet de loi définit « fournisseur de services électroniques » de façon très large, incluant les individus ainsi que les entreprises telles que les fournisseurs d'accès Internet, les opérateurs téléphoniques, les fournisseurs de courriel, les plateformes de médias sociaux, les applications de messagerie et, potentiellement, *toute entité offrant des services en ligne au public canadien*.[36, 37]

En bref, le projet de loi C-22 s'applique essentiellement à toutes les communications non papier entre tous les Canadiens en tout temps, ainsi qu'à chaque individu et organisation qui rend l'information disponible sous forme électronique, numérique ou autrement intangible.

Si le projet de loi C-22 est adopté, le gouvernement fédéral aura le pouvoir d'ordonner aux fournisseurs de services électroniques de développer la capacité d'organiser et d'extraire des données pour l'examen des forces de l'ordre,[38] d'installer des dispositifs facilitant le transfert d'informations aux forces de l'ordre,[39] et de conserver les métadonnées des utilisateurs jusqu'à un an.[40]

Il est important de noter que le projet de loi C-22 abaisse le seuil pour l'accès légal aux informations et métadonnées des abonnés des utilisateurs, passant de « motifs raisonnables de *croire* » à « motifs raisonnables de *soupçonner* » – facilitant ainsi l'accès aux renseignements sensibles des abonnés par la police. Les juges pourront émettre des mandats de perquisition en fonction de la *possibilité* qu'un crime se produise, plutôt que de la probabilité qu'un crime se produise.

En ce qui concerne les exigences de conservation des métadonnées, Michael Geist, professeur de droit à l'Université d'Ottawa et président de la recherche au Canada, a déclaré :

> *« Enfouie dans la deuxième moitié du projet de loi C-22 se trouve une disposition accordant au gouvernement le pouvoir d'exiger que les « fournisseurs principaux » conservent des catégories de métadonnées, y compris les données de transmission, jusqu'à un an. Il s'agit d'une conservation obligatoire des métadonnées qui obligerait les fournisseurs de télécommunications et de services électroniques à stocker des informations sur les communications de tous leurs utilisateurs, peu importe si ces utilisateurs sont soupçonnés ou non. C'est l'un des outils les plus intrusifs en*

[36] Ibid.
[37] Le projet de loi C-22 définit « fournisseur de services électroniques » comme « une personne qui, individuellement ou au sein d'un groupe, fournit un service électronique, y compris dans le but de permettre les communications, et qui (a) fournit ce service à des personnes au Canada; ou (b) exerce tout ou partie de ses activités commerciales au Canada. » Deuxième partie, 2(1).
[38] Parlement du Canada. *Projet de loi C-22 : Loi relative à l'accès légal*. Deuxième partie, 5(2)(a)
[39] Parlement du Canada. *Projet de loi C-22 : Loi relative à l'accès légal*. Deuxième partie, 5(2)(a)
[40] Parlement du Canada. *Projet de loi C-22 : Loi relative à l'accès légal*. Deuxième partie, 5(3)(c)

matière de vie privée qu'un gouvernement puisse déployer, et l'expérience internationale suggère qu'il existe d'importants risques pour la vie privée. »[41]

Bien que les métadonnées, ou « données sur les données », ne reflètent pas le *contenu* de la communication, elles capturent le *contexte* de la communication – adresses IP des utilisateurs, heure d'accès, services utilisés, avec qui vous avez communiqué, fréquence et durée d'utilisation, etc. En tant qu'entrées dans des modèles computationnels sophistiqués, ces données suffisent souvent à révéler aux forces de l'ordre des comportements, des relations, des associations, des intérêts et des habitudes. Avec le temps, les forces de l'ordre peuvent construire un portrait incomplet mais néanmoins révélateur du *noyau biographique* d'une personne. Bien que les forces de l'ordre auraient toujours besoin d'une autorisation judiciaire pour exiger de telles données, avec un seuil légal plus bas pour le faire, cela expose tous les Canadiens à un risque accru d'une surveillance gouvernementale sans précédent des services numériques qu'ils utilisent.

Bien que le projet de loi C-22 n'ait pas été formulé comme une solution pour prévenir les fusillades de masse ou d'autres crimes spécifiques, le seuil légal abaissé pour obtenir les informations des abonnés et les métadonnées des utilisateurs que cette législation introduit accorderait néanmoins au gouvernement et aux forces de l'ordre des pouvoirs beaucoup plus larges pour extraire des informations des utilisateurs des fournisseurs de services électroniques. Et cela inclurait probablement des entreprises d'IA comme OpenAI.

Conclusion

Le Premier ministre Mark Carney, lors de sa visite à Tumbler Ridge en février, a déclaré : « Évidemment, tout ce que quiconque aurait pu faire pour empêcher cette tragédie ou de futures tragédies doit être fait » – une réaction compréhensible et humainement appropriée à toute fusillade de masse. Les Canadiens font face à la question difficile mais familière : comment atteindre le plus haut niveau de sécurité publique tout en respectant les libertés fondamentales et les droits à la vie privée des citoyens. La réponse d'Ottawa à une fusillade de masse dévastatrice, bien qu'isolée, ne peut pas être disproportionnée, surtout en ce qui concerne les libertés civiles de tous les Canadiens. Il ne devrait pas utiliser une tragédie humaine comme prétexte pour adopter des lois qui rapprochent le Canada d'un État de surveillance.

Les réponses politiques actuellement à l'étude – la nationalisation de l'intelligence artificielle, l'élargissement des mandats réglementaires sur les entreprises privées d'IA et l'élargissement des vastes pouvoirs d'accès légal par le projet de loi C-22 – mettront les

[41] Geist, Michael. « Les risques de confidentialité de l'accès légal : décrypter les exigences étendues de conservation des métadonnées du projet de loi C-22. » *Blogue de Michael Geist*. 17 mars 2026. https://www.michaelgeist.ca/2026/03/the-lawful-access-privacy-risks-unpacking-bill-c-22s-expansive-metadata-retention-requirements/

interactions privées des Canadiens avec les chatbots IA sous surveillance et contrôle de l'État. Bien que motivées par un événement tragique, ces propositions normaliseraient l'accès gouvernemental à l'information personnelle et à la pensée privée d'une manière qui viole les protections de la Charte concernant la vie privée, l'expression et l'autonomie.

Tout accès gouvernemental aux données privées des utilisateurs doit être soumis à des exigences rigoureuses de mandat et confiné aux circonstances où un tel accès est nécessaire pour faire face à des menaces graves, imminentes et crédibles. Plutôt que d'abaisser le seuil pour obtenir des mandats, comme le propose le projet de loi C-22, le Parlement devrait maintenir une norme élevée tout en s'assurant que le processus de mandats fonctionne avec suffisamment de rapidité et d'efficacité.

En même temps, ce rapport ne suggère pas que les entreprises d'IA ont les mains propres. Les systèmes d'IA d'aujourd'hui peuvent déduire des informations sensibles sur les utilisateurs au-delà de ce que les utilisateurs eux-mêmes divulguent, générant des profils et des analyses très précis que les utilisateurs n'anticipent ni ne contrôlent entièrement. Cela soulève des préoccupations légitimes en matière de vie privée qui pourraient justifier une réglementation gouvernementale soigneusement adaptée.

Les Canadiens sont donc pris entre des pressions concurrentes : l'expansion gouvernementale des capacités de surveillance au nom de la sécurité publique, et les entreprises privées d'IA qui récoltent des données personnelles au nom de l'innovation et de l'expérience consommateur. Comment naviguer entre ces pressions – sans éroder les libertés fondamentales – sera l'un des défis politiques majeurs de notre époque.

Un chemin de principe est possible. Le Parlement devrait :

- Résister aux appels à nationaliser ou contrôler de manière centralisée les systèmes d'IA
- Rejeter le projet de loi C-22 et ses dispositions sur la conservation des métadonnées et l'accès forcé
- Maintenir des exigences rigoureuses en matière de mandat pour tous les accès étatiques aux données personnelles, limitant cet accès aux circonstances impliquant des menaces graves, imminentes et crédibles

Les Canadiens ont besoin d'un cadre juridique et réglementaire qui préserve des espaces pour penser, explorer et communiquer librement – en étant assurés que leurs droits *garantis par la Charte* demeurent intacts.

Bibliographie

Bélisle-Pipon, Jean-Christophe. « Le danger a été signalé mais non signalé : ce que révèle la tragédie de Tumbler Ridge sur le vide de gouvernance de l'IA au Canada. » *The Conversation*. 26 février 2026. https://theconversation.com/danger-was-flagged-but-not-reported-what-the-tumbler-ridge-tragedy-reveals-about-canadas-ai-governance-vacuum-276718.

Betke, Carl. « Les origines et le développement des numéros d'assurance sociale au Canada par David H. Flaherty (critique). » *La Revue historique canadienne*. Consulté le 10 avril 2026. https://muse.jhu.edu/pub/50/article/571331/pdf .

Boynton, Sean. « Un projet de loi républicain vise la Loi sur la diffusion en ligne et menace de représailles. » *Global News*. Publié le 19 mars 2025. Consulté le 10 avril 2026. https://globalnews.ca/news/11738344/cusma-online-streaming-act-us-bill-tariffs/

Castaldo, Joe. « Le ministre de l'IA dit à OpenAI que les experts canadiens doivent évaluer les conversations ChatGPT signalées. » *The Globe and Mail*. 4 mars 2026. https://www.theglobeandmail.com/business/article-ai-minister-tells-altman-canadian-experts-must-assess-flagged-chatgpt/ Consulté le 10 avril 2026.

Cecco, Leyland. « Le Canada cherche des réponses auprès d'OpenAI pour ne pas avoir alerté la police après avoir suspendu le compte du tireur dans une école. » *The Guardian*. 23 février 2026. https://www.theguardian.com/world/2026/feb/23/openai-tumber-ridge-shooter-account-suspended

Chatterji, Aaron, Cunningham, Deming, et al. « Comment les gens utilisent ChatGPT. » Bureau national de la recherche économique. Document de travail. Septembre 2025. https://www.nber.org/system/files/working_papers/w34255/w34255.pdf

Parlement européen. « Loi sur l'IA de l'UE : Premier règlement sur l'intelligence artificielle. » Consulté le 10 avril 2026. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Geist, Michael. « Une histoire de deux projets de loi : l'accès légal revient avec des changements à l'accès sans mandat, mais des risques dangereux de surveillance dérobée demeurent. » *Blogue de Michael Geist*. 13 mars 2026. https://www.michaelgeist.ca/2026/03/a-tale-of-two-bills-lawful-access-returns-with-changes-to-warrantless-access-but-dangerous-backdoor-surveillance-risks-remains/.

Geist, Michael. « Les risques de confidentialité de l'accès légal : décrypter les exigences étendues de conservation des métadonnées du projet de loi C-22. » *Blogue Michael Geist*. 17 mars 2026. https://www.michaelgeist.ca/2026/03/the-lawful-access-privacy-risks-unpacking-bill-c-22s-expansive-metadata-retention-requirements/.

Gouvernement du Canada. Ministère de la Justice. *Projet de loi C-2 : Loi concernant certaines mesures relatives à la sécurité de la frontière entre le Canada et les États-Unis et concernant*

d'autres mesures de sécurité connexes. Énoncé de charte. Consulté le 10 avril 2026. https://www.justice.gc.ca/eng/csj-sjc/pl/Charter-charte/c2_2.html.

Gouvernement du Canada. Innovation, Sciences et Développement économique Canada. « Le gouvernement du Canada lance un groupe de travail sur la stratégie IA et l'engagement public pour le développement de la prochaine stratégie IA. » 26 septembre 2025. https://www.canada.ca/en/innovation-science-economic-development/news/2025/09/government-of-canada-launches-ai-strategy-task-force-and-public-engagement-on-the-development-of-the-next-ai-strategy.html.

Hunter, Justine et Joe Castaldo. « OpenAI affirme que les récents changements de politique auraient signalé les messages du tireur de Tumbler Ridge à la police. » *The Globe and Mail*. 26 février 2026. https://www.theglobeandmail.com/canada/article-openai-chatgpt-tumbler-ridge-shooter-reporting-policies-changes/. Consulté le 10 avril 2026.

Carpay, John. « La Cour fédérale confirme sa décision contre l'utilisation gouvernementale de la Loi sur les situations d'urgence. » Centre juridique pour les libertés constitutionnelles, tel que publié sur le *Western Standard*. 16 janvier 2026. https://www.jccf.ca/western-standard-freedom-wins-again-federal-court-upholds-ruling-against-trudeaus-emergencies-act-overreach/. Consulté le 10 avril 2026.

Hannaford, Nigel. *Expansion de la mission : Est-il temps d'abolir le CRTC?* Centre juridique pour les libertés constitutionnelles. 23 mars 2026. https://www.jccf.ca/wp-content/uploads/2026/03/Mission-creep-Is-it-time-to-abolish-the-CRTC_Final_March-21-2026-1.pdf.pdf.

Hannaford, Nigel. *Effondrement de la vie privée et l'expansion de l'État de surveillance*. Centre juridique pour les libertés constitutionnelles. 24 février 2026. https://www.jccf.ca/wp-content/uploads/2026/02/Privacy-collapse-and-the-expanding-surveillance-state_FINAL.pdf.

Malik, Aisha. « ChatGPT atteint 900 millions d'utilisateurs actifs hebdomadaires » *TechCrunch*. 27 février 2026. https://techcrunch.com/2026/02/27/chatgpt-reaches-900m-weekly-active-users/

Bureau du commissaire à la protection de la vie privée du Canada. *Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA)*. Consulté le 10 avril 2026. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

Parlement du Canada. *Projet de loi C-22 : Loi relative à l'accès légal*. 45e Parlement, 1re session. Première lecture. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-22.

Parlement du Canada. *Projet de loi C-8 : Loi modifiant certaines lois et apportant certains amendements consécutifs (mise en œuvre de la Charte numérique)*. 45e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-8.

Parlement du Canada. *Projet de loi C-11 : Loi sur la diffusion en ligne*. 44e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-11

Parlement du Canada. *Projet de loi C-18 : Loi sur les nouvelles en ligne*. 44e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-18

Parlement du Canada. *Projet de loi C-2 : Loi relative à certaines mesures relatives à la sécurité publique et à la sécurité nationale*. 45e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-2.

Parlement du Canada. Projet de loi C-74 : *Loi sur la modernisation des techniques d'enquête*. 38e Parlement, 1re session. Consulté le 10 avril 2026. https://www.parl.ca/DocumentViewer/en/38-1/bill/C-74/first-reading

Pillay, Tharin. « Bots de soutien à l'intelligence émotionnelle IA. » *Time Magazine*. 19 février 2026. Consulté le 10 avril 2026. https://time.com/7379564/ai-emotional-intelligence-support-bots/.

Pruden, Jana G., Matthew Scace et Alanna Smith. « Unis dans le deuil : une communauté soudée de Tumbler Ridge se serre les coudes face à une tragédie 'inimaginable'. » T*he Globe and Mail*. Publié le 13 février 2026. Consulté le 28 avril 2026. https://www.theglobeandmail.com/canada/article-tumbler-ridge-community-tragedy-school-shooting/

Sanders, Nathan E. et Bruce Schneier. « OpenAI a montré qu'on ne peut pas lui faire confiance. Le Canada a besoin d'une IA publique et nationalisée. » *Schneier on Security*. 1er mars 2026. https://www.schneier.com/essays/archives/2026/03/openai-has-shown-it-cannot-be-trusted-canada-needs-nationalized-public-ai.html

Singh, Divyadeep. « La société mère de ChatGPT, OpenAI, a banni le compte du tireur scolaire de Tumbler Ridge, en Colombie-Britannique, a envisagé d'alerter la police canadienne, mais a retenu pour cette raison. » *The Economic Times*. 21 février 2026. https://economictimes.indiatimes.com/news/international/canada/chatgpts-parent-company-openai-banned-tumbler-ridge-b-c-school-shooters-account-mulled-alerting-canadian-police-but-held-back-over-this-reason/articleshow/128636101.cms

Cour suprême du Canada. R. c. Duarte, [1990] 1 R.C.S. 30.

Cour suprême du Canada. R. c. Marakah, 2017 SCC 59, [2017] 2 S.C.R. 608.

Cour suprême du Canada. R. c. Reeves, 2018 SCC 56, [2018] 3 S.C.R. 531.

Cour suprême du Canada. R. c. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212.

Cour suprême du Canada. *Saskatchewan (Commission des droits de la personne) c. Whatcott*, 2013 SCC 11, [2013] 1 R.C.S. 467.

Le groupe FDR. « Effets dissuasifs : la surveillance de la NSA pousse les écrivains américains à s'autocensurer. » Écrivez à l'Amérique. 12 novembre 2013. https://pen.org/report/chilling-effects/

Tumilty, Ryan. « Le ministre canadien de l'IA annonce qu'OpenAI va changer ChatGPT après la fusillade de Tumbler Ridge. » *The Star*. 6 mars 2026. https://www.thestar.com/politics/federal/canada-s-ai-minister-says-openai-to-change-chatgpt-after-tumbler-ridge-shooting/article_0c5daccf-e6dd-4bfd-b657-6e154a5caf23.html. Consulté le 10 avril 2026.

Woolf, Marie. 25 février 2026. « Ottawa avertit d'une législation si OpenAI n'apporte pas de changements après que l'historique des discussions ait déclenché des signaux d'alarme. » *The Globe and Mail*. 25 février 2026. https://www.theglobeandmail.com/politics/article-openai-justice-minister-legislation-tumbler-ridge-shooter-chat-history/