

— 5 août 2026

La Loi sur les réseaux sociaux sécuritaires :

**Une menace à notre
vie privée et à notre
liberté d'expression**

Censure, identification
obligatoire pour tous,
Internet contrôlé par
gouvernement

Auteur : Nigel Hannaford

**RECONNAISSANCE
FACIALE**



Centre juridique
pour les libertés constitutionnelles

Nous défendons
la liberté
au Canada

Résumé

Le Centre juridique pour les libertés constitutionnelles (CJLC) soutient l'objectif de protéger les enfants contre les préjudices en ligne. Le projet de loi C-34, la *Loi sur la sécurité des médias sociaux*, poursuit cet objectif par des mesures qui limitent injustement les droits et libertés *garantis par la Charte*. Une interdiction des réseaux sociaux pour les moins de 16 ans obligerait chaque Canadien à fournir une pièce d'identité ou une vérification d'âge, ou les deux, violant ainsi les droits à la vie privée de millions d'adultes et déplaçant l'autorité parentale. Des obligations vagues pour atténuer le « contenu nuisible » et réglementer les chatbots IA inciteront à la surcensure et mineront la liberté d'expression. Une nouvelle Commission de la sécurité numérique, exerçant des pouvoirs vastes et largement indéfinis sans véritable responsabilité envers le Parlement, créera de nouvelles règles, ordonnera le retrait de contenu et imposera de lourdes sanctions. Le Parlement devrait rejeter le projet de loi C-34 et plutôt se concentrer sur des mesures alternatives pour atténuer les préjudices aux enfants en ligne, y compris une meilleure application des dispositions existantes du *Code criminel* qui protègent déjà les enfants et les adultes contre les préjudices en ligne.

Droits d'auteur et réimpression

Droits d'auteur © 2026 Centre juridique pour les libertés constitutionnelles.

Sous licence Creative Commons <https://creativecommons.org/licenses/by-nc-nd/4.0/CC-BY-NC-ND>. <https://creativecommons.org/licenses/by-nc-nd/4.0/> Cette licence permet aux réutilisateurs de copier et de distribuer le matériel dans n'importe quel support ou format sous une forme non adaptée seulement, à des fins non commerciales uniquement, et seulement tant que l'attribution est donnée au créateur.



Remerciements

Nous remercions les milliers de Canadiens qui continuent de soutenir le Centre juridique pour les libertés constitutionnelles grâce à leurs dons. Leur générosité donne au Centre juridique pour les libertés constitutionnelles 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 1.0 de ce rapport, qui peut être mise à jour périodiquement.

Auteurs

L'auteur principal de ce rapport est Nigel Hannaford, un journaliste chevronné et analyste en politiques publiques.

Sommaire

Résumé exécutif	4
Une interdiction des réseaux sociaux pour les Canadiens de moins de 16 ans	7
<i>Charte</i> Section 8 Droit d'être protégé contre une fouille ou une saisie déraisonnable	9
<i>Charte</i> Section 7 Droit à la vie, à la liberté et à la sécurité	10
<i>Charte</i> Article 2(b) liberté d'expression	11
Réglementation des chatbots IA et devoirs de modération de contenu	12
Surveillance des conversations et divulgation à la police	12
Régulation des sorties des chatbots IA	13
La Commission de sécurité numérique : surveillance gouvernementale d'Internet	14
Composition et responsabilités	14
Règles encore à rédiger, sans contribution du Parlement	15
Recommandations	16
Bibliographie	17
Annexe A	19



Résumé exécutif

Le projet de loi C-34 du gouvernement fédéral, la *Loi sur les médias sociaux sécuritaires*, est présenté comme une mesure visant à protéger les enfants contre les préjudices en ligne. Elle imposerait un contrôle d'identité pour tous les Canadiens utilisant les médias sociaux, faciliterait une surveillance étendue des conversations privées avec IA et créerait un nouveau régulateur puissant avec une autorité largement indéfinie pour censurer la parole. Ces mesures limitent injustement les droits des Canadiens à la vie privée, à la liberté d'expression et à l'autorité parentale en vertu de la *Charte canadienne des droits et libertés*.

Le projet de loi C-34 stipulerait :

- Exiger des exploitants de sites pornographiques qu'ils mettent en place une vérification d'âge ou une estimation d'âge « adéquate » pour y accéder, et imposer des obligations visant à rendre inaccessibles le matériel d'abus sexuel sur enfants et les images intimes non consenties
- Interdire aux Canadiens de moins de 16 ans d'avoir des comptes sur certaines plateformes de médias sociaux, appliqué par des mesures « adéquates » de vérification et d'estimation de l'âge
- Imposer des obligations non spécifiées de conception, de sécurité, de surveillance et d'intervention en cas de crise aux services de chatbots IA conversationnelles; et
- Attribuer des pouvoirs larges et indéfinis à une nouvelle Commission canadienne de la sécurité numérique, y compris le pouvoir d'interpréter des normes vagues et d'imposer de lourdes sanctions aux plateformes non conformes.

Exiger une vérification d'âge rigoureuse pour les sites pornographiques spécialisés est une mesure ciblée et défendable. L'interdiction des réseaux sociaux pour les moins de 16 ans ne l'est pas. L'expérience d'autres pays, y compris l'interdiction australienne des réseaux sociaux pour les moins de 16 ans, montre que l'empêchement des mineurs d'accéder aux plateformes réglementées nécessite un dépistage de tous les utilisateurs.

Les plateformes en Australie ont utilisé l'estimation de l'âge facial, l'inférence comportementale et des vérifications « optionnelles » plus fortes, y compris la carte d'identité gouvernementale. Malgré tout, la plupart des moins de 16 ans ont continué d'utiliser les réseaux sociaux trois mois après l'interdiction, et la sensibilisation parentale à l'utilisation par les enfants a diminué pour certains groupes.

Une interdiction effective mènerait presque certainement à exiger que tous les Canadiens prouvent leur identité lorsqu'ils accèdent aux médias sociaux pour leur travail quotidien, leurs loisirs, leur éducation et leur exploration. Ce régime viole *les droits à la vie privée de l'article 8 de la Charte* pour des millions d'adultes : contraindre la remise de

renseignements d'identification hautement personnels comme condition de la vie quotidienne en ligne constitue une « perquisition ou saisie » illégale. C'est une mesure brutale, à l'échelle de la population, visant les enfants mais imposée à tous.

Le même régime remplace l'autorité parentale. La Cour suprême a reconnu que l' intérêt à la liberté de l'article 7 de *la Charte* inclut l'intérêt d'un parent à prendre des décisions fondamentales concernant la garde et l'éducation de ses enfants. Toute ingérence de l'État dans ce droit doit être soigneusement adaptée, et non arbitraire. Le projet de loi C-34, cependant, impose un système uniforme d'interdiction et de vérification à toutes les familles, sans évaluation individualisée ni possibilité pour les parents de décider que des méthodes moins restrictives suffisent. Une loi qui laisse la plupart des adolescents en ligne tout en rendant de nombreux parents moins informés sape à la fois la protection de l'enfance et l'autorité parentale.

Le projet de loi C-34 restreint également la liberté d'expression en vertu *de l'article 2(b) de la Charte*. Les plateformes de médias sociaux réglementées doivent mettre en place des mesures « adéquates » pour atténuer le risque que les utilisateurs soient exposés à du « contenu nuisible », y compris la catégorie vague de contenu qui « foment la haine ». Les lois criminelles et sur les droits humains existantes s'attaquent déjà à la signification de « haine », et ces normes sont elles-mêmes contestées. Le problème distinctif du projet de loi C-34 est qu'une nouvelle Commission, non élue – capable d'imposer de graves conséquences financières – aurait le pouvoir d'interpréter et d'appliquer des normes vagues sur les réseaux sociaux.

Face à de lourdes sanctions, les plateformes auront des incitatifs à retirer de façon excessive l'expression légitime d'opinions des Canadiens. Plusieurs des catégories les plus graves de « contenu nuisible », en particulier la victimisation sexuelle d'enfants et les images intimes non consenties, se chevauchent déjà largement avec *les infractions du Code criminel*. Là où les préjudices les plus graves sont déjà criminels, un régime administratif parallèle avec des seuils plus bas pour protéger *les droits et libertés garantis par la Charte* est difficile à justifier.

Les règles du projet de loi C-34 concernant les chatbots IA exigent que les opérateurs surveillent les conversations pour détecter des idées suicidaires, des automutilations ou l'intention de causer des dommages graves. Les opérateurs d'IA doivent interrompre ces discussions et peuvent les signaler aux services de crise ou à la police. Les opérateurs doivent créer des « plans de sécurité » numériques qui divulguent les critères pour référer les discussions à la GRC. Remplir ce devoir nécessite une surveillance à grande échelle des conversations privées. Les utilisateurs qui savent que leurs discussions peuvent être scannées, interrompues ou confiées aux autorités éviteront les sujets sensibles et controversés. Le projet de loi réglemente également les résultats des chatbots et les « comportements nuisibles », avec d'autres catégories laissées aux futures réglementations. Des normes floues et des sanctions sévères pousseront les entreprises



vers des modèles aseptisés et un accès réduit à l'information. Certaines compagnies quitteront le Canada.

La Commission de la sécurité numérique (DSC), créée par le projet de loi C-34, combinera les rôles réglementaires, d'enquête, d'adjudication et de plaider. Il peut contraindre des témoignages et des documents; Ses inspecteurs peuvent exiger des informations sans mandat. Plus important encore, 50 décisions majeures – y compris quels médias sociaux sont couverts, quelles méthodes de vérification d'âge sont acceptables et comment les normes vagues sont interprétées – sont laissées à la Commission ou au Cabinet après l'adoption du projet de loi. On demande au Parlement d'approuver une nouvelle architecture juridique sans savoir à quoi elle ressemblera en pratique. Le rapport annuel ne fournit qu'une responsabilité minimale. Le contrôle judiciaire existe en théorie, mais peu de Canadiens ordinaires peuvent se permettre de contester les règles ou sanctions de la Commission devant les tribunaux.

Le projet de loi C-34 crée donc un cadre qui sacrifie la vie privée, l'expression et l'autorité parentale *protégées par la Charte* pour des gains incertains. La protection de l'enfance est un objectif légitime. Elle n'exige pas de vérification obligatoire de l'identité de la population adulte, de devoirs ouverts pour atténuer la « haine », de surveiller les conversations sur l'IA de tous les Canadiens, ni de transférer des choix politiques fondamentaux du Parlement à un organisme non élu avec des garanties faibles.

Les interdictions *existantes du Code criminel* traitent déjà des préjudices en ligne les plus graves impliquant des enfants et des images intimes non consenties. Ces lois devraient être appliquées plus efficacement. Une responsabilité civile plus claire pour les choix de conception des plateformes qui nuisent prévisiblement aux enfants, et une vérification ciblée de l'âge pour la pornographie, sont des outils plus adaptés que la vérification à l'échelle de la population et une nouvelle Commission aux pouvoirs illimités.

Le Centre juridique pour les libertés constitutionnelles exhorte le Parlement à rejeter le projet de loi C-34. Les Canadiens devraient contacter leur député et exiger que la protection des enfants soit poursuivie par une meilleure application des lois existantes et des mesures qui respectent *les droits garantis par la Charte*, l'autorité parentale et le contrôle parlementaire sur l'élaboration des lois.

Une interdiction des réseaux sociaux pour les Canadiens de moins de 16 ans

Le projet de loi C-34, la *Loi sur la sécurité des médias sociaux*, crée une obligation légale sur certaines plateformes de médias sociaux de protéger les enfants et de réduire l'exposition des utilisateurs aux préjudices en ligne. Sans la participation du Parlement, le Cabinet fédéral décidera quelles plateformes de médias sociaux (par exemple, X, Facebook, YouTube, etc.) seront touchées.

L'article 27 interdit aux Canadiens de moins de 16 ans d'avoir un compte sur les plateformes de médias sociaux réglementées ou d'être autrement enregistrés par des mesures de vérification ou d'estimation de l'âge.¹ Les mesures de vérification et d'estimation de l'âge doivent être « efficaces »,² et les informations recueillies doivent être protégées, limitées à la vérification ou estimation de l'âge, et détruites une fois la vérification ou l'estimation terminée.³

L'article 28 permet au Cabinet d'imposer des règlements supplémentaires – qui ne seront créés qu'après l'adoption du projet de loi C-34 – afin de s'assurer que les Canadiens de moins de 16 ans ne puissent pas accéder aux plateformes de médias sociaux réglementées. En fait, cela donne au Cabinet un chèque en blanc pour ajouter des règles plus strictes après l'adoption du projet de loi, sans examen parlementaire. En vertu de l'article 29, une plateforme de médias sociaux peut être exemptée de certaines exigences si la Commission de la sécurité numérique est convaincue qu'elle offre déjà des « garanties adéquates » pour la protection des enfants.

En vertu de l'article 32, les plateformes de médias sociaux réglementées doivent mettre en place des mesures adéquates pour atténuer le risque que tous les utilisateurs de médias sociaux soient exposés à du contenu nuisible,⁴ presque tout étant déjà interdit par le *Code criminel*. Le projet de loi C-34 définit le contenu nuisible comme suit :

- a) du contenu intime communiqué sans consentement;
- b) du contenu qui victimise sexuellement un enfant ou revictimise un survivant;
- c) du contenu qui pousse un enfant à se faire du mal;
- d) du contenu utilisé pour intimider un enfant;
- e) du contenu qui attise la haine;
- f) du contenu qui incite à la violence; et

¹ Le projet de loi C-34 donne au Cabinet fédéral le pouvoir de décider (sans intervention du Parlement) quels médias sociaux seront ou non réglementés en vertu de la *Loi sur la sécurité des médias sociaux*.

² Projet de loi C-34, 1re session, 45e Parlement, 2026, art. 22(2).

<https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>.

³ Le projet de loi C-34, 1re session, 45e Parlement, 2026, art. 27(2)(c).

⁴ Projet de loi C-34, 1re session, 45e Parlement, 2026, art. 32(1).



g) Contenu sur le terrorisme ou l'extrémisme violent⁵

Le projet de loi C-34 ne précise pas comment la vérification de l'âge ou l'estimation sera réalisée. Les méthodes courantes incluent :

- Exiger que les utilisateurs soumettent une pièce d'identité émise par le gouvernement, des informations bancaires ou des dossiers médicaux;
- Utiliser des systèmes d'identification numérique gérés par le gouvernement;
- Recueillir des données biométriques (comme la reconnaissance faciale) pour estimer l'âge; ou
- Dédurre l'âge à partir du comportement et des habitudes d'activité des utilisateurs sur la plateforme.

Tout système efficace exigera presque certainement le dépistage de tous les Canadiens qui utilisent les médias sociaux, pas seulement ceux qui semblent avoir moins de 16 ans.

La *Loi australienne sur la sécurité en ligne* est entrée en vigueur en décembre 2025, interdisant aux mineurs de moins de 16 ans de détenir des comptes sur des plateformes de médias sociaux telles que *X, TikTok, Facebook, Instagram, Snapchat et Reddit*. Les plateformes de médias sociaux ont utilisé un mélange d'outils d'assurance de l'âge (y compris l'estimation de l'âge facial et l'inférence comportementale) et parfois des vérifications plus strictes. Bien que 4,7 millions de comptes non admissibles aient été supprimés de ces plateformes, l'interdiction restait loin d'atteindre son objectif.

Le commissaire à la sécurité électronique de l'Australie a rapporté en mars 2026 qu'environ sept parents sur dix dont les enfants avaient des comptes avant l'interdiction affirmaient que ces enfants avaient encore des comptes sur les principales plateformes.⁶ Le commissaire a jugé la mise en œuvre inadéquate et a poussé les plateformes à adopter des mesures plus robustes et continues, telles que de meilleurs modèles d'inférence et une escalade vers des vérifications plus fiables (y compris des vérifications d'identité bancaires ou « optionnelles »).⁷

Une mise à jour de juillet 2026 du commissaire a révélé que l'utilisation des réseaux sociaux par les moins de 16 ans n'avait fait que baisser de 85,9% à 81,5%.⁸ La conscience

⁵ Le projet de loi C-34, 1re session, 45e Parlement, 2026, art. 2(1) (définition de « contenu nuisible »).

⁶ Commissaire à la sécurité électronique. « Âge minimum sur les médias sociaux : mise à jour sur la conformité. » Mars 2026.
<https://www.esafety.gov.au/sites/default/files/202603/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf>.

⁷ La loi australienne interdit aux plateformes d'exiger strictement une pièce d'identité délivrée par le gouvernement ou une pièce d'identité numérique gouvernementale; cependant, cette méthode peut être proposée si elle est accompagnée d'une « alternative raisonnable ».

⁸ Cette mise à jour s'est concentrée sur la même période de rapport mais a fourni des données supplémentaires. « L'utilisation des médias sociaux » est différente de « compte sur les réseaux sociaux ».

des parents de la consommation par leurs enfants a également diminué pour certains groupes, en particulier les filles et les enfants âgés de 10 à 12 ans.⁹

Un régime qui laisse la plupart des adolescents en ligne tout en rendant certains parents moins conscients de ce que font leurs enfants sape à la fois la protection de l'enfance et l'autorité parentale.

Le droit de la Charte d'être protégé contre les fouilles ou saisies déraisonnables

Obliger les individus à fournir une pièce d'identité gouvernementale, des images faciales ou d'autres renseignements biométriques constitue une fouille ou une saisie en vertu de l'article 8 de la Charte. Dans l'affaire *Hunter c. Southam Inc.* (1984), la Cour suprême a statué que l'article 8 protège une attente raisonnable de vie privée partout où elle existe – y compris dans les données personnelles, les appareils et les communications – et que les fouilles doivent être raisonnables et, en règle générale, autorisées à l'avance.¹⁰ Dans *R. c. Duarte* (1990), la Cour a statué que la surveillance électronique secrète par l'État viole l'article 8, et que le gouvernement ne peut pas contourner cette protection en s'appuyant sur des intermédiaires pour obtenir des informations auxquelles il ne pourrait légalement pas accéder lui-même.¹¹ Dans l'affaire *R. c. Spencer* (2014), la Cour a statué que la police exige un mandat pour obtenir des informations sur les abonnés auprès d'un fournisseur d'accès Internet, même si ce dernier les divulgue volontairement.¹² Dans *R. c. Marakah* (2017), la Cour a statué que l'expéditeur d'un message texte conserve une attente raisonnable de vie privée même lorsque le message est stocké sur l'appareil d'une autre personne.¹³ Un régime qui oblige des millions d'adultes à remettre des données d'identification ou biométriques comme condition pour utiliser les médias sociaux quotidiens est une saisie large et indiscriminée imposée à chaque Canadien.

Si le projet de loi C-34 est adopté sous sa forme actuelle, il pourrait impliquer des documents émis par le gouvernement ou des données biométriques permanentes (ce que la Commission non élue et largement non responsable approuve comme « adéquate »). L'article 8 de la Charte est violé par une exigence large et indiscriminée imposant à des

⁹ eSafety Commissioner, « Premiers jours, premières perspectives : comprendre les expériences des restrictions d'âge sur les médias sociaux lors du suivi de trois mois », juillet 2026, <https://www.esafety.gov.au/sites/default/files/2026-07/Early-days-early-insights-SMMA-evaluation-three-months-July-2026.pdf>.

¹⁰ *Hunter et al. c. Southam Inc.*, [1984] 2 SCR 145, 1984 CanLII 33 (SCC). <https://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html>. Consulté le 18-06-2026.

¹¹ *R. c. Duarte*, [1990] 1 S.C.R. 30, 1990 CanLII 150 (SCC). <https://canlii.ca/t/1fszz>. Consulté le 18-06-2026.

¹² *R. c. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, 2014 CanLII 43 (SCC). <https://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html>. Consulté le 18-06-2026.

¹³ *R. c. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, 2017 CanLII 59 (SCC). <https://www.canlii.org/en/ca/scc/doc/2017/2017scc59/2017scc59.html>. Consulté le 18-06-2026.



millions d'adultes de remettre des informations d'identification hautement sensibles afin d'accéder aux plateformes de médias sociaux qu'ils utilisent chaque jour pour le travail, les loisirs et l'exploration.

Tel qu'il est rédigé actuellement, le projet de loi C-34 exige que les plateformes de médias sociaux « assurent la protection des renseignements personnels recueillis à des fins de vérification ou d'estimation d'âge jusqu'à ce que ces informations soient détruites. » L'inclusion de cette disposition reconnaît implicitement que les mesures contraintes de vérification de l'âge comportent des risques pour la vie privée des Canadiens. Il s'agit d'une mesure d'atténuation des risques – pas préventive. En l'absence de catastrophe d'une violation grave et irréversible de la vie privée, personne ne saura si l'information privée a réellement été détruite (ou correctement protégée avant sa destruction).

Aucune entreprise n'est entièrement protégée contre les violations de données. Par exemple, malgré la mise en place de mesures de protection des données, Bell Canada a subi quatre violations depuis 2016, Rogers Communications en a eu trois depuis 2015, LifeLabs en a eu une, et d'autres exemples abondent.¹⁴

L'article 7 de la *Charte* garantit le droit à la vie, à la liberté et à la sécurité de la personne

En imposant une interdiction générale des médias sociaux pour les moins de 16 ans, appliquée par une vérification d'âge obligatoire à chaque utilisateur de médias sociaux, le projet de loi C-34 place le gouvernement fédéral dans le rôle de parent. Dans *l'affaire B.(R.) c. Children's Aid Society of Metropolitan Toronto*,¹⁵ la majorité de la Cour suprême a statué que l'intérêt à la liberté protégé par l'article 7 inclut l'intérêt d'un parent à prendre des décisions fondamentales concernant la garde et l'éducation de ses enfants. Bien que cet intérêt ne soit pas absolu et doive s'appliquer lorsque la vie ou la santé d'un enfant est démontrée et imminemment en danger, la Cour a insisté pour que toute ingérence de l'État sur cet intérêt soit « soigneusement élaborée, adaptable à une multitude de situations différentes et loin d'être arbitraire. »¹⁶

Le projet de loi C-34 ne répond à aucune de ces exigences. Elle impose un régime uniforme d'interdiction et de surveillance à toutes les familles canadiennes, peu importe la maturité de l'enfant, la capacité des parents ou les risques réels présents dans un foyer donné. Il n'y a aucune occasion pour une famille de démontrer que des mesures moins restrictives

¹⁴ Corbado. « 11 plus grandes violations de données au Canada [2026]. » 14 avril 2025.

<https://www.corbado.com/blog/data-breaches-canada>.

15 B. (R.) c. Société d'aide à l'enfance du Grand Toronto, [1995] 1 R.C.S. 315.

<https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1220/index.do>. Consulté le 18-07-2026.

¹⁶ Ibid. à 383 (pour le juge La Forest).

suffisent, telles que les contrôles parentaux, les restrictions sur les appareils, l'éducation et un accès étroitement surveillé à Internet.

C'est l'opposé de l'intervention soigneusement adaptée, au cas par cas, requise par *B.(R.)*. Le projet de loi C-34 est un déplacement préventif et à l'échelle de la population de l'autorité parentale, appliqué grâce à une technologie atteinte à la vie privée qui n'a pas encore été établie, alors que sa nécessité et son efficacité restent inconnues. Les parents qui connaissent les vulnérabilités, le stade de développement et les habitudes en ligne de leurs propres enfants sont bien mieux placés pour prendre ces décisions qu'un régulateur fédéral éloigné.

Le droit à la liberté d'expression de l'article 2(b) de la Charte

Le projet de loi C-34 limite également fondamentalement la liberté des enfants et des adolescents de moins de 16 ans d'accéder à l'information et de s'exprimer via les médias sociaux. Cela viole la liberté d'expression protégée par l'article 2(b) de la *Charte*, qui protège à la fois le droit de parler ainsi que le droit d'entendre, lire et recevoir de l'information.

L'article 2(b) de la Charte est en outre violé par la large obligation des opérateurs de médias sociaux de réduire le risque que les utilisateurs soient exposés à du « contenu nuisible », ce qui inclut la catégorie vague et subjective du matériel « fomentant la haine ». ¹⁷ Les controverses publiques récentes illustrent à quel point cette norme peut facilement capter des opinions légitimes. Le fait de remettre en question le récit non fondé des meurtres dans les pensionnats ¹⁸ autochtones doit être qualifié de crime haineux, ou la justice d'une amende de 750 000 \$ infligée à un administrateur du conseil scolaire de Chilliwack pour avoir critiqué la politique du conseil de promouvoir l'idéologie transgenre auprès des enfants, ¹⁹ ce sont deux exemples.

Tel qu'écrit, le projet de loi C-34 donne à la Commission de la sécurité numérique le pouvoir de créer, d'interpréter et d'appliquer des normes, lui donnant le pouvoir effectif de juger certains points de vue « nuisibles » et de faire pression sur les plateformes pour les réprimer. Face à d'énormes amendes pour non-conformité, les plateformes auront de fortes incitations à sursupprimer ou à rétrograder algorithmiquement l'expression légitime

¹⁷ Section 2 (3) « Pour plus de certitude et aux fins de la définition *du contenu qui fomente la haine*, le contenu n'exprime pas de détestation ou de vilification uniquement parce qu'il exprime du mépris ou de l'antipathie ou parce qu'il discrédite, humilie, blesse ou offense. »

¹⁸ National Post. « Les chefs de l'AFN veulent que le négationnisme des pensionnats soit un crime de discours haineux. » 15 juillet 2026. <https://nationalpost.com/news/residential-school-denialism-hate-speech-crime-afn-chiefs>.

¹⁹ The Epoch Times. « Ancien administrateur contestera une amende de tribunal de 750 000 \$ à cause de propos anti-SOGI devant la Cour suprême de la Colombie-Britannique. » Février 2026. <https://www.theepochtimes.com/world/former-trustee-to-challenge-750k-tribunal-fine-over-anti-sogi-remarks-in-bc-supreme-court-5989949>.



de l'opinion. Cet effet dissuasif restreindra inévitablement *la liberté d'expression protégée par la Charte pour tous les Canadiens (de tous âges) qui utilisent les médias sociaux*.

De plus, la plupart des catégories de « contenu nuisible » du projet de loi C-34, en particulier celles impliquant la victimisation sexuelle d'enfants et les images intimes non consenties, sont déjà interdites par le *Code criminel*. Dans une affaire récente à Toronto, par exemple, un homme a été accusé de 68 infractions liées à des présumés incitatifs et exploitations d'enfants en ligne sur des plateformes telles que *Snapchat*, Instagram et *Discord*, y compris des abus sexuels sur enfants.²⁰ Lorsque le droit pénal interdit déjà les préjudices les plus graves, la restriction supplémentaire à la liberté d'expression n'est pas facilement justifiée comme une limite « raisonnable » aux *droits et libertés garantis* par la Charte.²¹

Réglementation des chatbots IA et devoirs de modération de contenu

Le projet de loi C-34 régit les entrées et les sorties des chatbots d'intelligence artificielle : ce qu'on peut dire à un chatbot et ce qu'un chatbot peut répondre en réponse.

La *Loi sur les médias sociaux sécuritaires* définit un « service de chatbot » comme un système d'intelligence artificielle accessible au public qui communique sur Internet et utilise un langage naturel pour fournir des réponses adaptatives, semblables à celles des humains, dans un format conversationnel. Les services de chatbot doivent aussi être capables de simuler une relation humaine durable à travers de multiples interactions ou sessions. La définition du projet de loi C-34 est suffisamment large pour potentiellement inclure des services tels que ChatGPT d'OpenAI, Grok de xAI et Gemini de Google.

Le projet de loi C-34 régit la façon dont les entreprises d'IA gèrent les conversations de chatbots impliquant des fantasmes de violence. Il s'agit vraisemblablement d'une réponse à la fusillade à l'école de Tumbler Ridge en février 2026.

Surveillance des conversations et divulgation à la police

De plus en plus, les Canadiens utilisent les chatbots IA non seulement pour la conversation, mais aussi pour la recherche, l'éducation et la découverte. Plus les

²⁰ CityNews. Service de police de Toronto / reportage : « Un homme de Toronto fait face à 68 accusations d'exploitation d'enfants en ligne avec des victimes présumées dans plusieurs pays. » 29 juillet 2026. <https://toronto.citynews.ca/2026/07/29/toronto-man-charged-online-child-exploitation/>.

²¹ En vertu de l'article 1 de la Charte, il incombe au gouvernement de justifier « de façon démontrable » avec des preuves convaincantes et convaincantes que sa violation d'un *droit ou d'une liberté fondée sur la Charte est raisonnable dans une « société libre et démocratique »*.

Canadiens dépendent des systèmes d'IA, plus le contrôle gouvernemental sur les résultats des chatbots devient important.

L'article 51 de la *Loi sur les médias sociaux sécuritaires* exigera que les services de chatbots réglementés interrompent immédiatement les discussions où les utilisateurs expriment des idées suicidaires, une intention d'automutilation ou une intention de commettre un acte pouvant causer la mort ou des blessures graves à une personne.

L'article 51 exige que les services de chatbot réfèrent ces conversations vers des « services d'intervention en cas de crise appropriés à la situation ». Le projet de loi C-34 ne fournit aucun cadre pour comprendre quel « service » (la GRC?) pourrait être approprié.

Un système ne peut pas identifier de façon fiable chaque conversation problématique sans examiner toutes les conversations. Les Canadiens seront observés lorsqu'ils exploreront légitimement l'histoire, la politique, la littérature, le terrorisme, les idéologies extrémistes, le crime et les enjeux de santé mentale. Lorsque les Canadiens savent que leurs discussions peuvent être scannées et interrompues (et potentiellement remises à la police), elles perdent la capacité de chercher librement de l'information et évitent souvent les sujets sensibles.

Les entreprises de chatbots réglementées devront également soumettre un « plan de sécurité numérique » à la Commission de la sécurité numérique divulguant les critères et processus du service pour faire passer à la GRC toute discussion où « il y a un risque qu'une personne commette un acte qui causerait la mort ou des blessures graves à une autre personne ».

Cela pourrait, à son tour, donner à la police un accès à des communications privées qu'elle aurait autrement besoin d'une autorisation judiciaire pour être obtenue, contrairement aux décisions de la Cour suprême du Canada selon lesquelles les individus maintiennent une attente raisonnable de vie privée dans leurs communications électroniques.²²

Régulation des sorties des chatbots IA

Le projet de loi C-34 réglemente également ce que les chatbots peuvent dire aux utilisateurs.

Les articles 49, 50 et 53 exigent que les services de chatbot réglementés mettent en place des mesures pour atténuer le risque de nuire aux utilisateurs. Les comportements nuisibles incluent le fait de se faire passer pour un être humain ou pour un professionnel médical, juridique ou autre professionnel agréé, manipuler les utilisateurs pour qu'ils développent des attachements émotionnels au chatbot, et encourager l'automutilation, le suicide ou des actes pouvant causer la mort ou des blessures graves à autrui. Il est

²² *R. c. Marakah*, 2017 SCC 59, [2017] 2 R.C.S. 608.



important de noter que l'article 53(e) étend cette obligation à « tout autre type de comportement spécifié dans les règlements ».²³ Ces règlements n'existent pas encore.

Ce que le Cabinet fédéral ou la Commission de la sécurité numérique détermineront à l'avenir comme « tout autre type » de production nuisible de chatbots aura des implications profondes pour l'accès des Canadiens à l'information.

L'article 53(e) se résume à « faire confiance au gouvernement ». Elle donne à une future Commission le pouvoir de réglementer une porte d'entrée de plus en plus importante vers l'information sans imposer de limites claires à l'autorité de cette Commission.

Face à de lourdes sanctions et à des obligations floues, les entreprises d'IA auront de puissants incitatifs à en conserver davantage, surveiller davantage, divulguer davantage et mettre en œuvre des modèles génératifs de plus en plus prudents. Sinon, ils peuvent simplement quitter le marché canadien.

Si le projet de loi C-34 est adopté sous sa forme actuelle, la réponse rationnelle pour les Canadiens sera de supposer que leurs conversations sur l'IA sont surveillées par des entreprises d'IA ou par la police. La réponse rationnelle pour les entreprises d'IA sera de pécher par excès de prudence au détriment de l'autonomie, de la liberté d'expression, de l'accès à l'information et de la vie privée des Canadiens.

La Commission de sécurité numérique : surveillance gouvernementale d'Internet

Le projet de loi C-34 établirait un nouvel organisme gouvernemental, la Commission de la sécurité numérique du Canada, pour faire respecter la conformité à la *Loi sur la sécurité numérique*. La Commission exercerait des pouvoirs substantiels de contrôle et de censure sur les plateformes de médias sociaux, les services de chatbots IA, les systèmes de vérification d'âge et d'identité, les pratiques d'atténuation de contenu et les fonctionnalités de conception utilisées pour protéger les enfants en ligne.

Composition et responsabilités

Les exploitants de services de médias sociaux, de services de chatbot et d'autres services en ligne à réglementer en vertu du projet de loi C-34 devront soumettre des plans de sécurité numérique expliquant leurs évaluations des risques, leurs garanties, leurs pratiques de conformité et l'allocation des ressources. La Commission examinera ces

²³ Projet de loi C-34, 1re session, 45e Parlement, 2026, articles 49, 50 et 53.

<https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>

informations pour évaluer la conformité, enquêter sur d'éventuelles infractions, accorder certaines exemptions, émettre des ordonnances et imposer des pénalités pécuniaires.

Lors de l'application de la *Loi sur les médias sociaux sécuritaires*, la Commission, largement non responsable, évaluera si les mesures adoptées par les entreprises sont « adéquates », y compris celles visant à atténuer l'exposition à des contenus nuisibles, à restreindre l'accès selon l'âge et à traiter les comportements nuisibles des chatbots. La Commission émettra des lignes directrices et établira des règlements ayant force de loi. Bien que la Commission doive soumettre un rapport annuel au Parlement, cette exigence de rapport n'offre qu'une responsabilité très limitée.

Le projet de loi C-34 donnerait à la Commission bon nombre des pouvoirs d'enquête et d'application habituellement associés à un tribunal ou à un grand tribunal réglementaire. En vertu de l'article 73, la Commission elle-même peut convoquer des témoins, les contraindre à témoigner sous serment et exiger la production de documents. En vertu de l'article 80, un inspecteur nommé par la Commission peut exiger que toute personne en possession d'un document ou d'une information le fournisse afin de vérifier la conformité. Aucun des deux pouvoirs ne requiert de mandat.

Si la Commission estime qu'un exploitant d'un service en ligne réglementé viole la législation, elle peut ordonner à cette entreprise de prendre – ou de s'abstenir – des mesures nécessaires à la conformité. Les ordonnances de la Commission peuvent être enregistrées auprès de la Cour fédérale et exécutées sous forme d'ordonnances judiciaires. En théorie, les ordonnances de la Commission peuvent être contestées devant les tribunaux, mais la plupart des entreprises n'auront pas les fonds nécessaires pour entamer un processus juridique très coûteux qui durera des années.

Enfreindre une disposition de la *Loi sur les médias sociaux sécuritaires* entraînera des sanctions allant jusqu'à 10 millions de dollars et trois pour cent du revenu brut mondial du délinquant. Ces sanctions créent de puissants incitatifs pour les entreprises réglementées à interpréter des exigences vagues de la manière la plus censureuse possible, avec peu ou pas de considération accordée aux droits à la vie privée et à la liberté d'expression des Canadiens.

Règles encore à rédiger, sans contribution du Parlement

Le professeur de droit de l'Université d'Ottawa, Michael Geist, estime qu'environ 50 questions importantes sont laissées à de futures réglementations ou décisions administratives de la Commission ou du Cabinet fédéral.²⁴ Cela inclut les seuils d'utilisation, les services réglementés, les exigences d'assurance d'âge, les

²⁴ Michael Geist. « La loi qui sera nommée plus tard : le projet de loi C-34 repousse 50 décisions clés au Cabinet et à une Commission de sécurité numérique qui n'existe pas encore. » Michael Geist (blogue), 11 juin 2026. <https://www.michaelgeist.ca/2026/06/the-law-to-be-named-later-bill-c-34-punts-50-key-decisions-to-cabinet-and-a-digital-safety-commission-that-does-not-yet-exist/>.



caractéristiques de conception pour les enfants, des mesures supplémentaires concernant la conduite des chatbots, ainsi que de nombreuses normes selon lesquelles la conformité des entreprises sera évaluée.²⁵

Dans le contexte d'un très grand gouvernement fédéral dont les dépenses annuelles dépassent 500 milliards de dollars par année,²⁶ le Parlement aura une influence pratique limitée sur les règles détaillées et les décisions d'application prises en vertu du projet de loi C-34.

Un résumé plus détaillé des pouvoirs différés et encore indéfinis de la Commission, préparé par le professeur Geist, est joint en annexe à ce document.²⁷

Recommandations

Le Centre de justice recommande que le Parlement :

1. **Rejeter le projet de loi C-34** dans sa forme actuelle.
2. **Appliquer *plus efficacement les interdictions* existantes du Code criminel** plutôt que d'imposer un régime administratif parallèle qui viole *les droits et libertés de la Charte avec la menace de sanctions énormes*.
3. **Préserver la vérification ciblée de l'âge pour accéder à la pornographie**, ce qui est une mesure plus restreinte et plus défendable qu'une interdiction aux moins de 16 ans sur les plateformes générales de médias sociaux imposée par le contrôle de tous les utilisateurs.
4. **Explorez des outils de droit civil** qui imposeraient une responsabilité aux entreprises qui facilitent directement ou indirectement l'accès à la pornographie et à d'autres préjudices en ligne, plutôt que d'étendre le contrôle gouvernemental sur Internet.
5. **Doter les parents** d'outils de soutien, d'éducation et de contrôles au niveau familial, plutôt qu'un régime fédéral uniforme d'interdiction et de surveillance qui traite chaque ménage de la même façon.
6. **Gardez les règles fondamentales d'expression en ligne, de vie privée et d'assurance de l'âge entre les mains des législateurs élus**, et non sous le contrôle d'une commission gouvernementale largement irresponsable.

²⁵ Geist, « The Law to Be Named Later », note 24 ci-dessus.

²⁶ Secrétariat du Conseil du Trésor du Canada. Estimations 2025–26. <https://www.canada.ca/en/treasury-board-secretariat/services/planned-government-spending/government-expenditure-plan-main-estimates/2025-26-estimates.html>.

²⁷ Voir Geist, « The Law to Be Named Later », note 24 ci-dessus. Un résumé des décisions reportées est joint en annexe A.

Les Canadiens devraient contacter leur député et exiger que la protection des enfants soit poursuivie par des mesures respectant la liberté d'expression, l'accès à l'information, la vie privée, l'autorité parentale et le contrôle parlementaire sur la législation.

Bibliographie

Législation

Canada. Parlement. Chambre des communes. *Projet de loi C-34, Loi visant à adopter la Loi sur la sécurité numérique et la Loi sur la Commission de la sécurité numérique du Canada et à apporter des modifications consécutives à d'autres lois*. 45e Parlement, 1re session. Première lecture, 10 juin 2026. <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-34/first-reading>.

Jurisprudence

B. (R.) c. Société d'aide à l'enfance du Grand Toronto, [1995] 1 R.C.S. 315. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1220/index.do>. Consulté le 18-06-2026.

Hunter et al. c. Southam Inc., [1984] 2 S.C.R. 145, 1984 CanLII 33 (SCC). <https://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html>. Consulté le 18-06-2026.

R. c. Duarte, [1990] 1 S.C.R. 30, 1990 CanLII 150 (SCC). <https://canlii.ca/t/1fszz>. Consulté le 18-06-2026.

R. c. Marakah, 2017 SCC 59, [2017] 2 R.C.S. 608. <https://www.canlii.org/en/ca/scc/doc/2017/2017scc59/2017scc59.html>. Consulté le 18-06-2026.

R. c. Spencer, 2014 SCC 43, [2014] 2 R.C.S. 212. <https://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html>. Consulté le 18-06-2026.

Sources secondaires

Geist, Michael. « La Commission : Comment le projet de loi C-34 crée un super-régulateur Internet qui touchera la vie de millions de Canadiens. » *Michael Geist* (blogue), 15 juin 2026. <https://www.michaelgeist.ca/2026/06/thecommission/>.

CityNews. « Homme de Toronto face à 68 accusations d'exploitation infantile en ligne avec des victimes présumées dans plusieurs pays. » 29 juillet 2026. <https://toronto.citynews.ca/2026/07/29/toronto-man-charged-online-child-exploitation/>.

Corbado. « 11 plus grandes violations de données au Canada [2026]. » 14 avril 2025. <https://www.corbado.com/blog/data-breaches-canada>.

Commissaire à la sécurité électronique. « Premiers jours, premières perspectives : comprendre les expériences des restrictions d'âge sur les réseaux sociaux lors du suivi de trois mois. » Juillet 2026. <https://www.esafety.gov.au/sites/default/files/2026-07/Early-days-early-insights-SMMA-evaluation-three-months-July-2026.pdf>.



Commissaire à la sécurité électronique. « Âge minimum sur les médias sociaux : mise à jour sur la conformité. » Mars 2026.

<https://www.esafety.gov.au/sites/default/files/202603/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf>.

The Epoch Times. « Ancien administrateur contestera une amende de tribunal de 750 000 \$ à cause de propos anti-SOGI devant la Cour suprême de la Colombie-Britannique. » Février 2026.

<https://www.theepochtimes.com/world/former-trustee-to-challenge-750k-tribunal-fine-over-anti-sogi-remarks-in-bc-supreme-court-5989949>.

Geist, Michael. « La Commission : Comment le projet de loi C-34 crée un super-régulateur Internet qui touchera la vie de millions de Canadiens. » Michael Geist (blogue), 15 juin 2026.

<https://www.michaelgeist.ca/2026/06/thecommission/>.

Geist, Michael. « La loi qui sera nommée plus tard : le projet de loi C-34 repousse 50 décisions clés au Cabinet et à une Commission de sécurité numérique qui n'existe pas encore. » Michael Geist (blogue), 11 juin 2026. <https://www.michaelgeist.ca/2026/06/the-law-to-be-named-later-bill-c-34-punts-50-key-decisions-to-cabinet-and-a-digital-safety-commission-that-does-not-yet-exist/>.

National Post. « Les chefs de l'AFN veulent que le négationnisme des pensionnats soit un crime de discours haineux. » 15 juillet 2026. <https://nationalpost.com/news/residential-school-denialism-hate-speech-crime-afn-chiefs>.

Documents gouvernementaux supplémentaires cités

Secrétariat du Conseil du Trésor du Canada. Estimations 2025–26.

<https://www.canada.ca/en/treasury-board-secretariat/services/planned-government-spending/government-expenditure-plan-main-estimates/2025-26-estimates.html>.

Annexe A

BILL C-34 · THE SAFE SOCIAL MEDIA ACT

The Law to Be Named Later

Bill C-34 punts 50 key decisions to cabinet and a Digital Safety Commission that does not yet exist

$$19 \text{ cabinet decision points in the Digital Safety Act} + 31 \text{ Commission regulation-making powers in s. 126(1)} = 50 \text{ key issues left to be decided after the bill becomes law}$$

Cabinet Decides

19 GOVERNOR IN COUNCIL DECISION POINTS

New categories of regulated online services	s. 5(1)
User thresholds: which social media services are regulated	s. 6(2)
Designating below-threshold social media services	s. 6(3)
User thresholds: which chatbot services are regulated	s. 7(2)
Designating below-threshold chatbot services	s. 7(3)
User thresholds: regulated online services	s. 8(2)
Designating below-threshold online services	s. 8(3)
Designating the responsible minister	s. 13
Requiring Commission hearings or reports on any matter	s. 19
Which services face the under-16 ban	s. 27(5)
Which services face prescribed under-16 measures	s. 28(3)
Criteria for exemptions from the under-16 ban	s. 29(2)
Enforcement mechanics: penalty factors, revenue, undertakings	s. 112
Cost-recovery charges to fund the Commission	s. 125(1)
AI systems excluded from the chatbot definition	s. 127(1)(a)
Defining "significant psychological or physical harm"	s. 127(1)(b)
Replacing the 24-hour takedown period (operator-identified)	s. 127(1)(c)
Replacing the 24-hour takedown period (user-flagged)	s. 127(1)(d)
Coming into force of the entire Act	s. 130

AND THAT'S NOT ALL

Not counted: seven more cabinet decisions under the Digital Safety Commission of Canada Act — appointing the members, designating the chair, fixing the head office and remuneration, and bringing both Acts into force.

Also not counted: the Commission's four guideline powers (ss. 16, 17, 24, 30), its rules of procedure, and its case-by-case adequacy determinations, exemption rulings, and orders.

The Commission Decides

31 HEADS OF REGULATION-MAKING POWER · S. 126(1)

Information required for user-threshold determinations	(a)
Child-protection design features and parental controls	(b)
Adequate age verification requirements	(c)
Measures limiting children's exposure to pornography	(d)
Record-keeping scope and retention	(e)
Measures preventing under-16 accounts	(f)
Factors for adequacy assessments	(g)
Additional adequacy and complaint-screening factors	(h)
Mandated mitigation measures (incl. upload prevention)	(i)
User guidelines	(j)
User blocking tools	(k)
Flagging tools and processes	(l)
Synthetic content labelling criteria	(m)
Bot-amplified content labelling	(n)
The mandatory resource person role	(o)
Preserving removed terrorism and incitement content	(p)
Digital safety plans: timing and reporting period	(q)
Digital safety plans: required information	(r)
Digital safety plans: additional information	(s)
Digital safety plans: publication	(t)
Takedown, representations, and reconsideration process	(u)
New types of prohibited chatbot harmful behaviour	(v)
Electronic data inventories in chatbot safety plans	(w)
Researcher accreditation	(x)
Researcher access to data inventories	(y)
Researcher data access requests	(z)
Data access conditions: privacy, IP, security	(z.1)
Revoking or amending data access orders	(z.2)
Complaint case management	(z.3)
Operator duties after Commission orders	(z.4)
Publication of violation notices by violators	(z.5)

Source: Bill C-34, the Safe Social Media Act (Digital Safety Act, enacted by s. 2)

michaelgeist.ca



Justice Centre
for Constitutional Freedoms