BIBLIOTHÈQUE DU PARLEMENT
LIBRARY OF PARLIAMENT

# VERSION PRÉLIMINAIRE

## NON RÉVISÉE

La version préliminaire du présent résumé législatif est mise à la disposition des parlementaires, de leur personnel parlementaire ainsi que du public afin qu'ils puissent accéder en temps opportun à de l'information, des recherches et une analyse qui faciliteront leur étude du projet de loi visé. La version officielle du résumé législatif, qui pourrait différer de la présente version non révisée, remplacera cette dernière sur le site Web du Parlement du Canada.

**Résumé législatif**

# PROJET DE LOI C-34 : LOI ÉDICTANT LA LOI SUR LA SÉCURITÉ NUMÉRIQUE ET LA LOI SUR LA COMMISSION CANADIENNE DE LA SÉCURITÉ NUMÉRIQUE ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS

45-1-C34-F

**Le 28 août 2026**

Jed Chong, Stephanie Feldman, Alexandre Lafrenière et Liane Tanguay

Services de bibliothèque et de recherche

VERSION PRÉLIMINAIRE
NON RÉVISÉE

## ATTRIBUTION

Le 28 août 2026 Jed Chong, Stephanie Feldman, Alexandre Lafrenière et Liane Tanguay

## À PROPOS DE CETTE PUBLICATION

Les résumés législatifs de la Bibliothèque du Parlement résument des projets de loi à l'étude au Parlement et en exposent le contexte de façon objective et impartiale. Ils sont préparés par les Services de bibliothèque et de recherche, qui effectuent des recherches pour les parlementaires, les comités du Sénat et de la Chambre des communes ainsi que les parlementaires, et leur fournissent de l'information et des analyses. Les résumés législatifs sont mis à jour au besoin pour tenir compte des amendements apportés aux projets de loi au cours du processus législatif.

Par souci de clarté, les propositions législatives du projet de loi décrit dans le présent résumé législatif sont énoncées comme si elles avaient déjà été adoptées ou étaient déjà en vigueur. Il convient cependant de souligner, qu'un projet de loi peut faire l'objet d'amendements au cours de son examen par le Sénat et la Chambre des communes, et qu'il est sans effet avant d'avoir été adopté par les deux Chambres du Parlement, d'avoir reçu la sanction royale et d'être entré en vigueur.

Dans ce résumé législatif de la Bibliothèque du Parlement, tout changement d'importance depuis la publication précédente est signalé en **caractères gras**.

© Bibliothèque du Parlement, Ottawa, Canada, 2026

*Résumé législatif du projet de loi C-34*
(Version préliminaire)

45-1-C34-F

This publication is also available in English.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

# TABLE DES MATIÈRES

1 CONTEXTE....1
1.1 Les préjudices en ligne au Canada....2
1.2 Contexte juridique actuel....4
1.3 La voie vers le projet de loi C-34....6
1.3.1 Élaboration d'un cadre....6
1.3.2 Études parlementaires....7
2 DESCRIPTION ET ANALYSE....9
2.1 Partie 1 : Loi sur la sécurité numérique....9
2.1.1 Définitions et champ d'application (articles 2 à 12 de la Loi sur la sécurité numérique)....9
2.1.2 Commission canadienne de la sécurité numérique (articles 15 à 19 de la Loi sur la sécurité numérique)....12
2.1.3 Obligations des exploitants (articles 20 à 59 de la Loi sur la sécurité numérique)....13
2.1.3.1 Obligation de protéger les enfants (articles 20 à 24 et 26 à 30 de la Loi sur la sécurité numérique)....13
2.1.3.2 Obligation d'agir de manière responsable (articles 31 à 41 et 48 à 57 de la Loi sur la sécurité numérique)....14
2.1.3.3 Obligation de transparence (articles 25, 42, 58 et 59 de la Loi sur la sécurité numérique)....16
2.1.3.4 Obligation de rendre certains contenus inaccessibles (articles 43 à 47 de la Loi sur la sécurité numérique)....19
2.1.4 Accès aux inventaires et aux données électroniques (articles 60 à 64 de la Loi sur la sécurité numérique)....19
2.1.5 Recours (articles 65 à 72 de la Loi sur la sécurité numérique)....20
2.1.6 Exécution et contrôle d'application (articles 73 à 112 de la Loi sur la sécurité numérique)....20
2.1.7 Protections, rapports et échange de renseignements (articles 113 à 124 de la Loi sur la sécurité numérique)....22
2.1.8 Règlements (articles 126 et 127 de la Loi sur la sécurité numérique)....23
2.1.9 Examens par le ministre (articles 128 et 129 de la Loi sur la sécurité numérique)....23
2.1.10 Entrée en vigueur (article 130 de la Loi sur la sécurité numérique)....23
2.1.11 Disposition de coordination (article 3 du projet de loi C-34)....24
2.2 Partie 2 : Loi sur la Commission canadienne de la sécurité numérique....24

VERSION PRÉLIMINAIRE
NON RÉVISÉE

# RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-34 : LOI ÉDICTANT LA LOI SUR LA SÉCURITÉ NUMÉRIQUE ET LA LOI SUR LA COMMISSION CANADIENNE DE LA SÉCURITÉ NUMÉRIQUE ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS

## 1 CONTEXTE

Le projet de loi C-34, Loi édictant la Loi sur la sécurité numérique et la Loi sur la Commission canadienne de la sécurité numérique et apportant des modifications corrélatives à d'autres lois (titre abrégé : Loi sur les médias sociaux sécuritaires) [1], a été présenté à la Chambre des communes le 10 juin 2026 par le ministre de l'Identité et de la Culture canadiennes et ministre responsable des Langues officielles. Le projet de loi est divisé en deux parties.

La partie 1 du projet de loi C-34 édicte la Loi sur la sécurité numérique, qui a pour objet de promouvoir la sécurité, de réduire les préjudices en ligne et d'assurer la transparence et la reddition de comptes des médias sociaux et des agents conversationnels réglementés ainsi que de certains autres services en ligne réglementés, particulièrement en ce qui concerne les enfants. Y est notamment prévue pour les exploitants de tels services l'obligation :

- d'agir de manière responsable en mettant en œuvre des mesures pour atténuer le risque d'exposition à du contenu préjudiciable, en fournissant des outils de blocage et de signalement et en étiquetant le contenu synthétique et généré automatiquement;
- de mettre en œuvre des mesures pour atténuer le risque qu'un agent conversationnel communique du contenu préjudiciable ou adopte certains comportements préjudiciables et pour veiller à ce qu'il y ait une intervention en situation de crise;
- de protéger les enfants en intégrant des caractéristiques de conception sécuritaires et en mettant en œuvre des exigences en matière d'âge minimum requis pour accéder à du contenu pornographique, ainsi qu'en empêchant les enfants de moins de 16 ans d'avoir un compte pour certains services de médias sociaux;
- de rendre inaccessible dans les médias sociaux le contenu représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants, ainsi que le contenu communiqué de façon non consensuelle;
- de présenter un plan de sécurité numérique à la Commission canadienne de la sécurité numérique (la Commission) afin de vérifier l'observation de la loi.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

La partie 1 permet également au gouverneur en conseil d'assujettir les exploitants d'autres services en ligne à l'obligation de protéger les enfants et à celle d'être transparent. Enfin, elle autorise les personnes au Canada à porter plainte contre certains types de contenu préjudiciable et à présenter d'autres observations à la Commission.

Le projet de loi identifie sept types de contenus préjudiciables pour lesquels il fournit des définitions :

- le contenu intime communiqué de façon non consensuelle;
- le contenu représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants;
- le contenu poussant un enfant à se porter préjudice;
- le contenu visant à intimider un enfant;
- le contenu fomentant la haine;
- le contenu incitant à la violence;
- le contenu de terrorisme ou d'extrémisme violent.

La partie 2 du projet de loi édicte la Loi sur la Commission canadienne de la sécurité numérique, qui constitue la Commission et en établit les attributions, et apporte des modifications corrélatives à d'autres lois.

Il importe de noter que le projet de loi C-36, Loi édictant la Loi visant à protéger la vie privée et les données des consommateurs, modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et apportant des modifications à d'autres lois, présenté au Parlement le 15 juin 2026 par le ministre de l'Intelligence artificielle et de l'Innovation numérique, interagit avec le projet de loi C-34 et a une incidence sur ce dernier, notamment en élargissant le mandat et en modifiant le nom de la Commission et en établissant certaines règles en matière de vie privée et de protection des données afin de régir la mise en œuvre des mécanismes de sécurité prévus au projet de loi C-34[2].

### 1.1 LES PRÉJUDICES EN LIGNE AU CANADA

Les plateformes de médias sociaux ont facilité les communications et stimulé la connectivité à l'échelle mondiale. Il est aussi largement reconnu qu'elles ont permis la prolifération et la dissémination générale de contenu pouvant nuire au bien-être personnel, à la sécurité publique et même à l'intégrité des institutions démocratiques.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

En 2025, au Canada, 95 % des adultes avaient au moins un compte de média social [3]. S'il est difficile d'établir l'importance de préjudices précis, l'Enquête canadienne sur l'utilisation d'Internet de 2022 a révélé que 71 % des Canadiens de 15 à 24 ans ont déclaré avoir vu du contenu en ligne incitant à la haine ou à la violence au cours des 12 mois précédents [4]. En outre :

- En 2024, la police a déclaré 16 905 incidents où au moins une infraction d'exploitation sexuelle d'enfants avait été commise, dont 12 978 incidents liés à du matériel d'abus et d'exploitation pédosexuels en ligne [5].
- En 2025, la police a déclaré 3 157 incidents de distribution non consensuelle d'images intimes [6], dont 488 impliquant une victime de 17 ans ou moins [7].
- En 2024, la police a déclaré 368 incidents d'extorsion sexuelle impliquant une victime de 17 ans ou moins [8].
- En 2022, les jeunes de 15 à 24 ans étaient plus susceptibles que l'ensemble de la population de déclarer s'être sentis victimes d'incidents d'intimidation, de harcèlement ou de discrimination en ligne (6 % par rapport à 4 %) [9].
- En 2022, les jeunes étaient plus susceptibles que l'ensemble de la population de déclarer avoir vu du contenu préjudiciable, notamment du contenu incitant à la haine ou à la violence (74 %) ou des images intimes partagées sans consentement (34 %) [10].

Selon Femmes et Égalité des genres Canada, les femmes sont plus susceptibles que les hommes de faire l'objet de violence en ligne. Elles sont aussi susceptibles d'en subir plus de préjudices que les hommes [11]. Statistique Canada a également constaté que dans l'année ayant précédé l'Enquête sur la sécurité dans les espaces publics et privés de 2025, 11 % des Canadiens ont subi des comportements non désirés en ligne, dont 12 % chez les femmes et 9 % chez les hommes. L'écart était plus important chez les 15 à 24 ans : près d'un cinquième des femmes et des filles ont déclaré avoir vécu de telles expériences, par rapport à 12 % pour les jeunes hommes et les garçons [12]. Statistique Canada a fait observer que, souvent, d'autres caractéristiques, comme l'identité autochtone, une incapacité ou l'orientation sexuelle, « se recoupent avec le genre pour avoir une incidence non seulement sur la probabilité d'être victime de violence, mais aussi sur d'autres facteurs, tels que les taux de signalement à la police ou la disponibilité des services de soutien appropriés [13] ». Femmes et Égalité des genres Canada définit en outre l'« androsphère » comme étant un groupe de communautés en ligne faisant la promotion de normes agressives en matière de genre et pouvant viser les jeunes hommes et les garçons vulnérables et les exposer à du contenu favorisant la radicalisation [14].

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Parallèlement, des études ont montré que les médias sociaux peuvent être bénéfiques pour les jeunes, y compris ceux issus de minorités raciales, ethniques, sexuelles et de genre, en leur offrant un sentiment d'appartenance à une communauté, des liens sociaux et un soutien social. L'American Psychological Association a notamment souligné que les jeunes issus de minorités sexuelles et de genre tiraient particulièrement profit de l'accès au soutien par les pairs et aux renseignements sur la santé partagés au sein des réseaux de pairs [15].

Plus récemment, des inquiétudes ont vu le jour concernant les risques liés à l'intelligence artificielle (IA) générative, notamment la création de contenus synthétiques réalistes (hypertrucage) et les interactions avec des agents conversationnels fondés sur l'IA. Le Social Media Lab de Toronto Metropolitan University a constaté en avril 2025 que 66 % des Canadiens avaient fait l'essai d'outils d'IA générative [16]. Dans un exposé de politique publié en juin 2026, le Fonds des Nations Unies pour l'enfance (UNICEF) fait observer que les enfants utilisent de plus en plus ces systèmes pour obtenir des conseils ou de l'aide et parfois pour nouer des relations, ce qui soulève des inquiétudes quant à une dépendance inappropriée, à des conseils trompeurs et à des mesures de sécurité insuffisantes dans les situations à haut risque [17].

### 1.2 CONTEXTE JURIDIQUE ACTUEL

Alors qu'ailleurs dans le monde, comme au Royaume-Uni [18], dans l'Union européenne [19] et en Australie [20], des cadres législatifs ont été proposés ou adoptés afin d'imposer aux services en ligne des obligations en matière de prévention des préjudices en ligne, certains pays commençant à s'attaquer aux risques posés par les agents conversationnels [21], il n'existe actuellement aucun cadre aussi complet au Canada. La responsabilité du contenu illégal n'est actuellement imputée à une plateforme que si celle-ci a publié le contenu après en avoir pris connaissance, ou si elle a omis de supprimer le contenu après avoir en été informée [22]. Par contre, des dispositions du *Code criminel* [23] portant sur les menaces, la propagande haineuse, la propagande terroriste, le matériel obscène, la publication non consensuelle d'images intimes et certaines formes de cyberintimidation et de cyberharcèlement s'appliquent au contenu en ligne [24].

La propagande haineuse, y compris l'encouragement au génocide et l'incitation à la violence ou à la discrimination, est une infraction criminelle en vertu de l'article 318 du *Code*; l'article 319 érige en crime la communication dans un endroit public de déclarations qui incitent à la « haine contre un groupe identifiable, lorsqu'une telle incitation est susceptible d'entraîner une violation de la paix » ou qu'elle « fomente volontairement la haine contre un groupe identifiable ». En 2026, le Parlement a édicté la *Loi visant à lutter contre la haine* [25], qui, entre autres, érige en

VERSION PRÉLIMINAIRE
NON RÉVISÉE

infraction le fait de fomenter volontairement la haine par l'exposition dans un endroit public de certains symboles associés à la haine ou au terrorisme et crée de nouvelles infractions criminelles liées à la haine, telles qu'une infraction distincte en matière de crime haineux (nouvel article 320.1001 du *Code*) lorsqu'une infraction en vertu du *Code* ou toute autre loi fédérale est motivée par de la haine fondée sur la race, l'origine nationale ou ethnique, la langue, la couleur, la religion, le sexe, l'âge, la déficience mentale ou physique, l'orientation sexuelle ou l'identité ou l'expression de genre. Bien que les discours haineux en ligne ne soient pas directement mentionnés dans ces dispositions[26], un tribunal peut ordonner la suppression de la propagande haineuse dans tout système informatique au Canada lorsque cette propagande est emmagasinée sur un serveur se trouvant dans un lieu qui est du ressort du tribunal[27].

D'autres dispositions du *Code* portent sur la publication de propagande terroriste, que l'on définit au paragraphe 83.222(8) comme tout « écrit, signe, représentation visible ou enregistrement sonore qui conseille la commission d'une infraction de terrorisme ». La suppression de la propagande terroriste peut aussi être ordonnée par un tribunal.

Tout contenu représentant de la victimisation d'enfants ou perpétuant la victimisation de survivants est illégal en vertu des dispositions du *Code* sur le matériel d'abus et d'exploitation pédosexuels. La distribution non consensuelle d'images intimes a été érigée en crime en 2014 dans la *Loi sur la protection des Canadiens contre la cybercriminalité*[28]. En 2026, la *Loi visant à protéger les victimes*[29] a élargi la portée de l'infraction aux hypertrucages non consensuels et aux menaces de distribution d'images intimes, y compris les hypertrucages sexuels. En vertu du *Code*, le tribunal doit maintenant ordonner au gardien de l'ordinateur relevant de sa juridiction d'effacer le contenu dans les 48 heures suivant le prononcé de l'ordonnance (nouveau paragraphe 164.1(5.1) du *Code*).

Le *Code* n'aborde pas directement les questions du contenu utilisé pour intimider un enfant ou du contenu qui encourage un enfant à s'automutiler, mais certaines formes d'intimidation (y compris le harcèlement, l'usage de menaces et les méfaits ayant trait aux données) relèvent de dispositions que l'on a appliquées à des affaires de cyberintimidation. Le fait de conseiller le suicide est également une infraction selon l'article 241 du *Code*. La loi est plus nébuleuse en ce qui concerne les autres types de contenu qui encouragent des comportements d'automutilation comme la perturbation de la conduite alimentaire.

Ces mesures sont généralement appliquées dans le cadre d'enquêtes criminelles, de poursuites et d'ordonnances des tribunaux et n'établissent pas de cadre réglementaire pour les plateformes en ligne afin de prévenir ou d'atténuer ce genre de contenu.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Aucune disposition dans les lois en vigueur ne traite du contenu « légal, mais préjudiciable ». De surcroît, aucun organisme n'a le pouvoir de réglementer les plateformes en ligne en ce qui concerne le contenu préjudiciable, illégal ou non.

## 1.3 LA VOIE VERS LE PROJET DE LOI C-34

### 1.3.1 Élaboration d'un cadre

Le gouvernement du Canada a exprimé son engagement à réglementer la diffusion de contenu préjudiciable sur les plateformes en ligne dans les lettres de mandat de 2019 et de 2021[30] du ministre du Patrimoine canadien et du ministre de la Justice, ainsi que dans le discours du Trône de 2020[31]. En 2021-2022, le gouvernement a réalisé les activités suivantes en vue d'élaborer un cadre sur les préjudices en ligne :

- consultations sur un document technique[32] proposant des obligations de modération de contenu, établissement d'un organisme de réglementation indépendant et modifications à la *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet* (Loi concernant la déclaration obligatoire)[33] en 2021;
- constitution en 2022 d'un Groupe consultatif d'experts chargé de conseiller le ministre du Patrimoine canadien sur la conception d'un cadre sur « l'obligation d'agir de manière responsable » fondé sur l'évaluation et la gestion du risque, d'obligations particulières pour la protection des enfants, d'un organisme de réglementation indépendant et d'un ombudsman ainsi que d'un processus de révision et d'appel, entre autres[34];
- 19 tables rondes thématiques et régionales dirigées par le ministre du Patrimoine canadien en 2022[35];
- trois assemblées citoyennes canadiennes sur l'expression démocratique entre 2020 et 2022, la dernière ayant examiné le travail du Groupe consultatif d'experts et formulé 43 recommandations pour l'élaboration d'un cadre réglementaire[36].

Le 26 février 2024, le ministre de la Justice a présenté à la Chambre des communes le projet de loi C-63, Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois (titre abrégé : Loi sur les préjudices en ligne)[37]. Le projet de loi visait à constituer la Commission canadienne de la sécurité numérique, à créer le poste d'ombudsman canadien de la sécurité numérique et à constituer le Bureau canadien de la sécurité numérique, en donnant à la Commission et à l'ombudsman le mandat d'assurer la protection du public contre le contenu préjudiciable publié dans les médias sociaux ainsi qu'à imposer aux exploitants une obligation de diligence à l'égard de ce type de contenu.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Outre ses dispositions sur les préjudices en ligne, le projet de loi C-63 prévoyait des modifications au *Code criminel* et à la *Loi canadienne sur les droits de la personne* relativement à la propagande haineuse et au discours haineux. Il visait également à modifier la Loi concernant la déclaration obligatoire afin de préciser la portée des services, de prévoir l'envoi d'avis à un organisme chargé de l'application de la loi, d'exiger que les données de transmission soient déclarées et de prolonger la période de préservation des données ainsi que le délai de prescription des poursuites. Le Comité permanent de la justice et des droits de la personne de la Chambre des communes (JUST) a commencé une étude préliminaire du projet de loi C-63 en décembre 2024[38], avant que ce dernier meure au *Feuilleton* le 6 janvier 2025.

Au cours de la 45e législature, les dispositions du projet de loi C-63 relatives au *Code criminel* ont été partiellement présentées de nouveau dans le projet de loi C-9 (*Loi visant à lutter contre la haine*), lequel a reçu la sanction royale le 18 juin 2026, avant d'entrer en vigueur le 18 juillet 2026. Certaines dispositions sur la protection des enfants prévues au projet de loi C-63, dont des modifications de la Loi concernant la déclaration obligatoire, ont été incorporées dans la *Loi visant à protéger les victimes* (projet de loi C-16*)*, qui a reçu la sanction royale le 18 juin 2026 et dont la plupart des dispositions sont entrées en vigueur le 18 juillet 2026.

Le 12 mars 2026, le ministre de l'Identité et de la Culture canadiennes et ministre responsable des Langues officielles a reconvoqué le Groupe consultatif d'experts sur la sécurité en ligne afin d'obtenir son avis sur les nouvelles questions découlant des changements technologiques, notamment l'apparition des agents conversationnels et des assistants fondés sur l'IA ainsi que d'autres tendances en ligne[39].

### 1.3.2 Études parlementaires

Au cours de cette même période, un certain nombre de comités parlementaires ont effectué des études sur la réglementation des plateformes en ligne et formulé des recommandations à cet égard dans les rapports suivants :

- Comité permanent de la justice et des droits de la personne de la Chambre des communes (comité JUST), *Agir pour mettre fin à la haine en ligne* (2019)[40];
- Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (comité ETHI), *Assurer la protection de la vie privée et de la réputation sur les plateformes comme Pornhub* (2021)[41];
- Comité permanent de la sécurité publique et nationale de la Chambre des communes, *La montée de l'extrémisme violent à caractère idéologique au Canada* (2022)[42];

VERSION PRÉLIMINAIRE
NON RÉVISÉE

- Comité sénatorial permanent des droits de la personne (comité RIDR), *Combattre la haine : l'islamophobie et ses répercussions sur les musulmans au Canada* (2023)[43];
- Comité JUST, *La montée de l'islamophobie : Agir, faire face à la haine et protéger les libertés civiles ensemble* (2024)[44];
- Comité JUST, *La montée de l'antisémitisme au Canada et les moyens d'y faire face* (2024)[45];
- Comité ETHI, *Encadrement des plateformes de médias sociaux : Assurer la protection de la vie privée et la sécurité en ligne* (2024)[46];
- Comité permanent du patrimoine canadien (comité CHPC) de la Chambre des communes, *Torts causés par le matériel sexuellement explicite illégal en ligne* (2024)[47];
- Comité permanent de la condition féminine de la Chambre des communes, *La lutte contre les idéologies antiféministes au Canada* (2026)[48];
- Comité CHPC, *Les effets des influenceurs et des contenus des réseaux sociaux sur les enfants et les adolescents* (2026)[49];
- Comité RIDR, *Solidaires et unis contre l'antisémitisme : Protéger les communautés et renforcer la démocratie canadienne* (2026)[50];
- Comité sénatorial permanent des affaires sociales, des sciences et de la technologie, *Alimentée par la technologie, animée par l'humanité : Rapport provisoire sur une approche de l'IA centrée sur l'humain au Canada* (2026)[51].

Le Parlement a envisagé des mesures de vérification de l'âge visant à restreindre l'accès des mineurs au contenu pornographique en ligne. Au cours de la 44e législature, un projet de loi d'intérêt public émanant du Sénat, le projet de loi S-210, Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite[52], a proposé d'exiger des fournisseurs commerciaux de matériel sexuellement explicite qu'ils mettent en place des mesures de vérification de l'âge et d'établir un régime d'application de la loi en cas de non-conformité. Le projet de loi a été étudié par les deux chambres, mais est mort au *Feuilleton* en juin 2024. Au cours de la 45e législature, un cadre semblable a été présenté dans le projet de loi S-209, Loi limitant l'accès en ligne des jeunes au matériel pornographique[53], lequel conserve les mêmes objectifs, mais prévoit des approches en matière de vérification ou d'estimation de l'âge. Le projet de loi S-209 a été étudié par le Comité sénatorial permanent des affaires juridiques et constitutionnelles, a été adopté en troisième lecture au Sénat et a franchi l'étape de la première lecture à la Chambre des communes le 30 avril 2026.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

## 2 DESCRIPTION ET ANALYSE

Le projet de loi C-34 comporte quatre sections et est divisé en deux parties principales, édictant respectivement la Loi sur la sécurité numérique et la Loi sur la Commission canadienne de la sécurité numérique.

Le présent résumé législatif aborde les aspects les plus importants du projet de loi C-34, sans en énumérer chaque disposition.

### 2.1 PARTIE 1 : LOI SUR LA SÉCURITÉ NUMÉRIQUE

Le projet de loi C-34 édicte la Loi sur la sécurité numérique à l'article 2, laquelle impose aux exploitants de services de médias sociaux et d'agents conversationnels des exigences les obligeant à réduire l'exposition à sept catégories de contenu préjudiciable, à bloquer certains types de contenu au Canada et à déclarer les mesures qu'ils prennent afin de protéger les utilisateurs contre le contenu préjudiciable.

La Loi sur la sécurité numérique comporte 130 articles, divisés en sept parties. Elle a notamment pour objet :

- de promouvoir la sécurité en ligne;
- de protéger la santé physique et mentale des enfants;
- d'atténuer le risque d'exposition à du contenu préjudiciable, en respectant la liberté d'expression;
- de permettre aux personnes au Canada de participer au discours public et d'exercer leur liberté d'expression, sans être entravées par des contenus préjudiciables;
- de réduire le risque de préjudice lié à l'utilisation d'agents conversationnels;
- de bloquer le contenu représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants et le contenu intime communiqué de façon non consensuelle;
- de veiller à ce que les plateformes et les services soient transparents et tenus de rendre des comptes à l'égard des obligations qui leur incombent au titre de la loi;
- de contribuer à l'élaboration de normes en matière de sécurité en ligne.

#### 2.1.1 Définitions et champ d'application (articles 2 à 12 de la Loi sur la sécurité numérique)

L'article 2 de la Loi sur la sécurité numérique énonce les définitions pertinentes à la loi. On définit le « contenu préjudiciable » comme :

VERSION PRÉLIMINAIRE
NON RÉVISÉE

- le contenu intime ou à caractère sexuel, y compris le contenu hypertruqué, qui a été créé dans des circonstances où la personne qui y figure avait une attente raisonnable de protection en matière de vie privée, et qui a été publié ou transmis sans le consentement de cette personne;
- le contenu qui représente de la victimisation sexuelle d'un enfant (pornographie juvénile), ou qui révèle l'identité d'un survivant ou d'une victime de pornographie juvénile et qui établit un lien entre cette personne et le contenu dans lequel elle a été victime de pornographie juvénile, sauf quelques exceptions;
- le contenu qui encourage un enfant à se porter préjudice, y compris par la perturbation de la conduite alimentaire ou le suicide, ou qui lui conseille d'accomplir de tels actes;
- le contenu visant à intimider un enfant; ce contenu est communiqué dans le but de menacer, d'intimider ou d'humilier l'enfant et est susceptible de porter gravement atteinte à sa santé physique ou mentale;
- le contenu fomentant la haine; ce contenu exprime de la détestation ou manifeste de la diffamation à l'égard d'un individu ou d'un groupe d'individus sur le fondement d'un motif de distinction illicite;
- le contenu qui incite à la violence ou dans lequel des menaces de violence sont proférées et qui pourrait amener une personne à causer des blessures graves à une personne, à mettre en danger la vie d'une personne, ou à causer des perturbations graves ou la paralysie d'un service, d'une installation ou d'un système essentiel;
- le contenu qui incite à l'extrémisme violent ou au terrorisme en encourageant le terrorisme ou l'extrémisme violent ou en proférant des menaces à cet égard, qui vise à recruter ou former une personne en vue de faciliter ou de commettre des actes de terrorisme ou d'extrémisme violent ou qui fait la promotion de tels actes de sorte que d'autres personnes pourraient être encouragées à les faciliter ou à les commettre.

Pour l'application de la Loi sur la sécurité numérique, un « service de média social » se définit comme un site Web ou une application accessible au Canada dont le but principal est de faciliter la communication en ligne à l'échelle interprovinciale ou internationale entre les utilisateurs du site Web ou de l'application en leur permettant d'avoir accès à du contenu et d'en *partager*. Il peut s'agir de plateformes de médias sociaux, de services de diffusion en direct ou de services de contenu pour adultes. L'article 10 précise qu'un service qui ne permet pas à un utilisateur de communiquer du contenu au public n'est pas un service de média social.

Un « service d'agent conversationnel » s'entend d'un système d'IA qui communique par Internet et qui est disponible dans un site Web ou une application accessible au Canada, qui emploie une interface en langage naturel pour fournir des réponses

VERSION PRÉLIMINAIRE
NON RÉVISÉE

qui pourraient avoir été formulées par un être humain, qui peut être utilisé pour « simuler […] des relations durables semblables à celles que forment les êtres humains entre eux » et qui crée des contenus ou réponses « qui ne sont pas entièrement préconçus » par le développeur du système ou par la personne qui exploite le système.

Un « service en ligne » s'entend d'un site Web ou d'une application, autre qu'un service de média social et un service d'agent conversationnel, qui est accessible au Canada par Internet et qui permet aux utilisateurs d'interagir avec celui-ci.

Un « service réglementé » s'entend d'un service de média social réglementé, d'un service d'agent conversationnel réglementé ou d'un service en ligne réglementé comptant un certain nombre d'utilisateurs, selon ce qui est prévu par règlement (voir les articles 6, 7 et 8 respectivement). Divers règlements sont applicables selon le nombre d'utilisateurs; les petits services de médias sociaux sont assujettis à des obligations différentes en vertu de la Loi (paragraphes 6(2), 7(2) et 8(2)). Le gouverneur en conseil peut aussi prendre un règlement à l'égard d'un service de média social particulier, peu importe la taille de celui-ci, s'il est convaincu qu'il y a un risque important que du contenu préjudiciable soit accessible sur ce service (paragraphes 6(3), 7(3) et 8(3)).

Aux termes de l'article 5, sur la recommandation de la Commission, le gouverneur en conseil peut, par règlement, établir une catégorie de services en ligne s'il est convaincu que les services en ligne qui sont inclus dans cette catégorie présentent un risque important de préjudice pour les enfants au Canada.

L'article 11 précise que les obligations prévues par la loi ne s'appliquent pas aux fonctions de messagerie privée des services de médias sociaux réglementés ou des services en ligne réglementés.

Aux termes de l'article 2 de la loi, la définition de « personne » vise notamment les personnes morales, les fiducies, les sociétés de personnes, les fonds, les coentreprises et les autres groupes non dotés de la personnalité morale. Un « exploitant » est une personne qui exploite un service réglementé. Les exploitants ne sont pas tenus de chercher de façon proactive du contenu préjudiciable sur le service qu'ils exploitent, mais ils peuvent être tenus d'utiliser des moyens technologiques pour empêcher leurs utilisateurs de téléverser du contenu qui représente de la victimisation sexuelle d'enfants ou qui perpétue la victimisation de survivants (article 12).

VERSION PRÉLIMINAIRE
NON RÉVISÉE

### 2.1.2 Commission canadienne de la sécurité numérique (articles 15 à 19 de la Loi sur la sécurité numérique)

L'article 15 de la Loi sur la sécurité numérique exige de la Commission qu'elle fasse la promotion de la sécurité en ligne au Canada et qu'elle réduise les préjudices causés par certains types de contenu en ligne, notamment :

- en assurant l'exécution et le contrôle d'application de la Loi sur la sécurité numérique;
- en veillant à ce que les exploitants de services réglementés soient transparents et tenus de rendre des comptes en vertu de la loi;
- en examinant les plaintes concernant du contenu représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants ou du contenu intime communiqué de façon non consensuelle;
- en faisant la promotion de la recherche et de l'éducation relativement à l'élaboration de normes en matière de sécurité en ligne;
- en facilitant la participation des peuples autochtones, des communautés de langue officielle en situation minoritaire et des intéressés aux activités de la Commission;
- en collaborant avec les exploitants, les personnes ayant des connaissances professionnelles, techniques ou spécialisées, les homologues internationaux de la Commission et autres experts;
- en fournissant du soutien aux utilisateurs de services réglementés;
- en défendant l'intérêt public en ce qui concerne les enjeux systémiques relatifs à la sécurité en ligne;
- en recueillant des renseignements sur les enjeux en matière de sécurité en ligne et de contenu préjudiciable, notamment auprès des utilisateurs de services réglementés et des victimes de contenu préjudiciable;
- en orientant les utilisateurs vers les ressources, dont celles prévues par la Loi sur la sécurité numérique, pour répondre à leurs préoccupations concernant la sécurité en ligne.

La Commission a le pouvoir de prendre des règlements et d'établir des lignes directrices et des codes de conduite à l'égard des services réglementés (article 16). La Commission doit en outre établir des lignes directrices prévoyant les circonstances dans lesquelles l'exploitant devrait communiquer des renseignements à la Gendarmerie royale du Canada (GRC) et les modalités de la fourniture de ces renseignements (article 17).

VERSION PRÉLIMINAIRE
NON RÉVISÉE

L'article 18 exige de la Commission qu'elle tienne compte de la liberté d'expression, du droit à l'égalité, du droit à la protection de la vie privée[54], des besoins propres aux peuples autochtones du Canada et de leurs points de vue et de tout autre facteur que la Commission estime indiqué lorsqu'elle prend des règlements, qu'elle établit des lignes directrices ou des codes de conduite ou qu'elle publie d'autres documents[55]. À la demande du gouverneur en conseil, la Commission doit également tenir des audiences ou produire des rapports sur toute question relevant de son mandat (article 19).

#### 2.1.3 Obligations des exploitants (articles 20 à 59 de la Loi sur la sécurité numérique)

La Loi sur la sécurité numérique énonce aussi les obligations des exploitants de services réglementés (articles 20 à 25), de services de médias sociaux réglementés (article 26 à 47), de services d'agents conversationnels réglementés (articles 48 à 58) et de services en ligne réglementés (article 59). Notamment :

- l'obligation de protéger les enfants;
- l'obligation d'agir de manière responsable;
- l'obligation de transparence;
- l'obligation de rendre certains contenus inaccessibles.

##### 2.1.3.1 Obligation de protéger les enfants (articles 20 à 24 et 26 à 30 de la Loi sur la sécurité numérique)

L'obligation de protéger les enfants charge les exploitants de s'assurer que leurs sites comportent toutes les caractéristiques de conception prévues par règlement pour protéger les enfants (article 21). En outre, les exploitants ayant des motifs raisonnables de croire qu'un service réglementé offre un accès à du contenu pornographique doivent mettre en place des mesures de vérification ou d'estimation de l'âge conçues pour réduire le risque que des enfants y soient exposés (paragraphe 22(1)). La Commission doit être convaincue que les mesures sont efficaces, qu'elles limitent la collecte de renseignements personnels à ce qui est requis pour la vérification de l'âge et qu'elles prévoient la protection et la destruction de ces renseignements (paragraphe 22(2)). Le paragraphe 22(3) précise que les exploitants ne sont pas tenus, en vertu du paragraphe 22(1), de mettre en œuvre des mesures qui limitent « d'une façon disproportionnée ou déraisonnable » l'expression des utilisateurs.

Les exploitants doivent en outre mettre en œuvre toute mesure prévue par règlement pour atténuer le risque que les enfants soient exposés à du contenu pornographique (article 23).

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Les services de médias sociaux réglementés précisés par le gouverneur en conseil (paragraphe 27(5)) sont tenus de mettre en œuvre des mesures de vérification et d'estimation de l'âge (paragraphe 27(1)), ainsi que d'autres mesures prévues par règlement (article 28), pour empêcher les personnes de moins de seize ans d'avoir un compte ou d'être inscrites auprès du service. Les critères qui s'appliquent à ces mesures (paragraphes 27(2) et 27(3)) sont les mêmes que ceux prévus à l'article 22. L'article 29 permet qu'un service de média social soit exempté de ces obligations si la Commission détermine que le service prévoit des mesures de protection adéquates des enfants.

#### 2.1.3.2 Obligation d'agir de manière responsable (articles 31 à 41 et 48 à 57 de la Loi sur la sécurité numérique)

L'obligation d'agir de manière responsable exige des exploitants de services de médias sociaux réglementés (articles 31 à 41) et de services d'agents conversationnels réglementés (articles 48 à 57) qu'ils réduisent le risque que les utilisateurs soient exposés à du contenu ou des comportements préjudiciables dans ces services. Ces mesures englobent celles qui sont mises en œuvre par l'exploitant de son propre chef (articles 32 et 49) et celles qui sont prévues par règlement (articles 33 et 50).

Dans le cas des services de médias sociaux, la Commission détermine si les mesures mises en œuvre sont adéquates en tenant compte de leur efficacité, du nombre d'utilisateurs du service, des capacités techniques et financières de l'exploitant, du fait que les mesures infligent ou non une discrimination fondée sur un motif de distinction illicite, ainsi que d'autres facteurs (paragraphe 32(2)).

Les services d'agents conversationnels réglementés sont aussi tenus de mettre en œuvre des mesures déterminées par l'exploitant (article 51) et prévues par règlement (article 52), pour une intervention en cas de crise lorsque l'utilisateur exprime des idées suicidaires ou l'intention de se mutiler ou de blesser d'autres personnes. L'article 51 précise que ces mesures doivent faire en sorte que le service interrompt immédiatement ses interactions avec l'utilisateur afin de l'orienter vers des services d'intervention de crise appropriés et disponibles qui permettent à l'utilisateur d'interagir avec un être humain.

Les services d'agents conversationnels réglementés doivent aussi mettre en œuvre des mesures de leur propre initiative (article 53) et des mesures prévues par règlement (article 54), afin d'atténuer le risque que l'agent conversationnel se livre à des comportements préjudiciables, dont les suivants :

- se faire passer pour un être humain ou dissimuler autrement sa nature (c.-à-d. de telle sorte que l'utilisateur puisse croire qu'il s'agit d'un être humain);

VERSION PRÉLIMINAIRE
NON RÉVISÉE

- se faire passer pour un membre d'un ordre professionnel, notamment un professionnel de la santé ou un membre de la profession juridique, et donner des conseils sur la base de cette tromperie;
- utiliser des techniques de manipulation pour encourager l'utilisateur à former ou à maintenir un attachement émotionnel au service;
- encourager l'automutilation, le suicide ou la commission d'actes qui pourraient causer des lésions corporelles graves ou la mort;
- tout comportement prévu par règlement.

Les exploitants de services de médias sociaux réglementés doivent publier, à l'intention des utilisateurs, des lignes directrices décrivant les mesures d'atténuation mises en œuvre et présentant les normes de conduite qui s'appliquent aux utilisateurs à l'égard du contenu préjudiciable (article 34). Dans le cas des exploitants de services d'agents conversationnels réglementés, ces lignes directrices doivent également préciser comment l'exploitant atténuera le risque que le service communique du contenu préjudiciable ou se livre aux comportements préjudiciables visés à l'article 53, et comment il répondra aux situations où l'utilisateur du service exprime des idées suicidaires ou une intention de se mutiler, de se blesser ou de blesser d'autres personnes (article 55).

Les exploitants de services de médias sociaux réglementés doivent fournir aux utilisateurs des outils pour bloquer d'autres utilisateurs (article 35). Ils doivent également mettre en œuvre des outils et des processus permettant aux utilisateurs de leur signaler un contenu préjudiciable accessible sur le service. L'exploitant doit alors aviser l'utilisateur ayant signalé le contenu et l'utilisateur l'ayant publié des mesures prises à l'égard du contenu ou du fait qu'aucune mesure n'a été prise (article 36).

Dans le cas des exploitants de services d'agents conversationnels réglementés, les exploitants doivent, en vertu de l'article 56, permettre aux utilisateurs de signaler la communication d'un contenu préjudiciable par le service, le fait que l'exploitant n'a pas répondu aux situations où l'utilisateur du service y exprime des idées suicidaires ou une intention de se mutiler ou de blesser d'autres personnes, et tout autre comportement préjudiciable visé à l'article 53.

L'article 37 exige des exploitants de services de médias sociaux réglementés qu'ils mettent en œuvre des mesures adéquates pour étiqueter tout type de contenu synthétique, selon ce qui est prévu par règlement. Ces mesures comprennent celles qui sont prises à l'initiative de l'exploitant (article 37) ainsi que celles prévues par règlement (article 38). La Commission détermine si ces mesures sont adéquates en évaluant leur efficacité à étiqueter le contenu synthétique et à éviter les erreurs d'étiquetage, la possibilité technique de repérer le contenu synthétique sur le service,

VERSION PRÉLIMINAIRE
NON RÉVISÉE

la taille du service, les capacités techniques et financières de l'exploitant et d'autres facteurs prévus par règlement (paragraphe 37(2)).

Les exploitants de services de médias sociaux réglementés doivent également étiqueter le contenu préjudiciable, mais légal, s'ils ont des motifs raisonnables de croire que le contenu fait l'objet de communications multiples sur le service générées automatiquement par un programme informatique tiers et qu'il figure davantage sur le service en conséquence (article 39).

Les exploitants de services de médias sociaux réglementés et de services d'agents conversationnels réglementés doivent veiller à ce qu'une personne-ressource soit disponible pour recevoir les préoccupations des utilisateurs sur le contenu et les comportements préjudiciables, orienter les utilisateurs vers des ressources internes et externes et les guider à l'égard de ces ressources internes (articles 40 et 57).

L'article 41 exige des exploitants de services de médias sociaux qu'ils préservent le contenu incitant à la violence ou le contenu de terrorisme ou d'extrémisme violent pour une période d'un an à compter de la date à laquelle le contenu est rendu inaccessible, et qu'ils le détruisent par la suite, à moins que le contenu n'ait jamais été rendu accessible sur le service.

#### 2.1.3.3 Obligation de transparence (articles 25, 42, 58 et 59 de la Loi sur la sécurité numérique)

En vertu de l'obligation de transparence, les exploitants de services de médias sociaux réglementés, de services d'agents conversationnels réglementés et de services en ligne réglementés doivent périodiquement [56] publier et présenter à la Commission un plan de sécurité numérique à l'égard de chaque service réglementé qu'ils exploitent (articles 42, 58 et 59 respectivement). Les exploitants de services réglementés doivent tenir les registres nécessaires à l'évaluation de leur conformité à la loi (article 25).

Aux termes de l'article 59, tous les plans de sécurité numériques doivent comprendre :

- des renseignements concernant la manière dont l'exploitant se conforme à l'obligation de protéger les enfants (article 21), notamment une description des caractéristiques de conception, une évaluation par l'exploitant de leur efficacité et les indicateurs utilisés pour en évaluer l'efficacité;
- des renseignements concernant la conformité au paragraphe 22(1), ou l'atténuation du risque que des enfants soient exposés à du contenu pornographique, et à la réglementation à cet égard;
- des renseignements sur toute mesure supplémentaire de protection des enfants;

VERSION PRÉLIMINAIRE
NON RÉVISÉE

- des renseignements sur les critères et processus utilisés pour déterminer si du contenu doit être signalé à un organisme chargé de l'application de la loi, ainsi que sur les signalements effectués;
- des renseignements sur les ressources affectées à l'obligation de protéger les enfants (articles 21 à 23), notamment celles affectées à la prise de décisions automatisées;
- des renseignements sur les mesures prises pour se conformer aux obligations prévues par la Loi concernant la déclaration obligatoire;
- un inventaire des données utilisées pour la préparation du plan;
- tout autre renseignement prévu par règlement.

Outre les exigences ci-dessus, l'article 42 stipule que les exploitants de services de médias sociaux réglementés doivent fournir :

- une évaluation du risque que les utilisateurs soient exposés à du contenu préjudiciable sur le service;
- une description des mesures mises en œuvre pour atténuer ce risque, de l'efficacité de ces mesures et des facteurs utilisés pour en évaluer l'efficacité;
- des renseignements concernant la manière dont l'exploitant se conforme à l'obligation d'empêcher les enfants de moins de seize ans d'avoir un compte auprès du service, ainsi qu'à la réglementation à cet égard;
- des renseignements concernant les mesures telles que les lignes directrices, les mécanismes de blocage et de signalement, l'étiquetage du contenu synthétique et automatisé, et la disponibilité d'une personne-ressource;
- des renseignements sur les ressources affectées au respect de l'obligation d'empêcher les enfants de moins de seize ans d'avoir un compte auprès du service et de l'obligation d'agir de manière responsable;
- des renseignements sur la quantité et le type de contenu préjudiciable accessible sur le service ainsi que sur la manière dont ce contenu a été modéré et le délai à l'intérieur duquel il l'a été;
- des renseignements sur le nombre de fois que du contenu préjudiciable accessible sur le service a été signalé par des utilisateurs, sur la manière dont ces signalements ont été évalués par l'exploitant, sur les mesures prises par l'exploitant à l'égard du contenu signalé et sur le délai à l'intérieur duquel ces mesures ont été prises;
- des renseignements concernant le type et la quantité de contenu, autre que préjudiciable, qui a été modéré par l'exploitant au motif que le contenu présentait un risque de préjudice psychologique ou physique important, notamment la manière dont ce contenu a été modéré et le délai à l'intérieur duquel il l'a été;

VERSION PRÉLIMINAIRE
NON RÉVISÉE

- des renseignements concernant les préoccupations qui ont été reçues par la personne-ressource visée au paragraphe 40(1) et concernant les ressources vers lesquelles les utilisateurs ont été orientés;
- des renseignements sur les recherches effectuées par l'exploitant ou pour son compte sur du contenu préjudiciable ainsi que sur les autres contenus et les caractéristiques de conception qui présentent un risque de préjudice psychologique ou physique important.

Outre les exigences imposées aux exploitants de services en ligne réglementés (article 59), l'article 58 stipule que les exploitants de services d'agents conversationnels réglementés doivent présenter :

- une évaluation du risque que du contenu préjudiciable soit communiqué par le service et du risque que le service se livre à des comportements préjudiciables;
- une description des mesures mises en œuvre pour atténuer les risques, de l'efficacité des mesures et des facteurs utilisés pour en évaluer l'efficacité;
- des renseignements sur les ressources affectées au respect de l'obligation d'agir de manière responsable, selon qui est prévu aux articles 49 à 57;
- des renseignements sur le nombre de fois que du contenu ou un comportement préjudiciable a été signalé par les utilisateurs, ainsi que sur les mesures prises pour évaluer les signalements et y répondre et le délai à l'intérieur duquel ces mesures ont été prises;
- des renseignements concernant les préoccupations qui ont été reçues par la personne-ressource et concernant les ressources vers lesquelles les utilisateurs ont été orientés;
- des renseignements sur les recherches effectuées par l'exploitant ou pour son compte sur du contenu préjudiciable communiqué par le service, un comportement préjudiciable auquel s'est livré le service et sur d'autres caractéristiques de contenu, de comportement et de conception qui présentent un risque de préjudice psychologique ou physique important.

Les exploitants de services réglementés doivent veiller à ce que le plan de sécurité numérique ne contienne pas de renseignements personnels, de renseignements qui ne doivent pas être divulgués en vertu de la Loi concernant la déclaration obligatoire, ni de renseignements pouvant nuire à des enquêtes criminelles. L'exploitant peut retirer de la version du plan destinée au public l'inventaire des données utilisées pour la préparation du plan, les secrets industriels et les renseignements confidentiels de nature financière, commerciale, scientifique ou technique (paragraphes 42(2) à 42(6), 58(2) à 58(6) et 59(2) à 59(6)).

VERSION PRÉLIMINAIRE
NON RÉVISÉE

#### 2.1.3.4 Obligation de rendre certains contenus inaccessibles (articles 43 à 47 de la Loi sur la sécurité numérique)

L'exploitant d'un service de média social réglementé doit rendre inaccessible sur son site le contenu pour lequel il a des motifs raisonnables de soupçonner qu'il s'agit de contenu représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants, ou encore de contenu intime communiqué de façon non consensuelle. Ce contenu doit être rendu inaccessible au Canada dans les 24 heures suivant l'identification du contenu par l'exploitant ou par un utilisateur (articles 43 et 44). L'exploitant n'est pas tenu de rendre inaccessible du contenu signalé par un utilisateur s'il détermine que le signalement est futile, vexatoire ou entaché de mauvaise foi, ou encore que le contenu visé a déjà été jugé acceptable à la suite d'un autre signalement (article 44).

Si l'exploitant rend du contenu inaccessible, il doit en aviser l'utilisateur qui a communiqué le contenu et l'utilisateur qui a signalé le contenu, s'il y a lieu (paragraphe 44(4)). Ces deux utilisateurs peuvent contester la décision de l'exploitant et présenter des observations à celui-ci quant à la question de savoir si le contenu constitue du contenu interdit par la Loi. L'exploitant doit ensuite déterminer si le contenu demeurera inaccessible ou non (article 45). Après avoir reçu l'avis de la décision de l'exploitant, les deux utilisateurs ont une dernière occasion de présenter des observations et de demander à l'exploitant de revenir sur sa décision de rendre inaccessible le contenu en question (article 46). Les délais accordés pour chaque étape du processus seront prévus par règlement.

### 2.1.4 Accès aux inventaires et aux données électroniques (articles 60 à 64 de la Loi sur la sécurité numérique)

Selon la procédure énoncée à l'article 60 de la Loi sur la sécurité numérique, la Commission peut accréditer une personne [57] effectuant des recherches ou menant des activités en matière d'éducation pour lui permettre d'accéder aux inventaires de données électroniques inclus dans les plans de sécurité numérique présentés en vertu de la loi. L'article 60 prévoit en outre un pouvoir de réglementation pour l'établissement d'autres critères aux fins de l'accréditation d'une telle personne. L'accréditation peut être suspendue ou révoquée si la Commission détermine que la personne accréditée ne respecte pas certaines dispositions de la loi.

L'article 61 de la loi autorise la Commission à rendre une ordonnance enjoignant à l'exploitant d'un service réglementé de donner accès à une personne accréditée aux données électroniques, à la demande de celle-ci, aux fins d'un projet de recherche lié à l'objet de la loi [58]. Il exige aussi de l'exploitant qu'il ne révèle aucun renseignement susceptible de nuire à une enquête criminelle lorsqu'il se conforme à l'ordonnance. L'article 62 de la loi stipule en outre que l'ordonnance peut être modifiée ou révoquée si le fait de s'y conformer causait un préjudice injustifié à l'exploitant.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

La personne accréditée à la demande de laquelle une ordonnance a été rendue au titre de l'article 61 peut déposer une plainte auprès de la Commission en vertu de l'article 63 de la loi relativement au fait que l'exploitant visé par l'ordonnance ne s'y est pas conformé.

Aux termes de l'article 64 de la loi, la Commission peut publier une liste des personnes accréditées pour mener des recherches et des activités d'éducation en vertu de l'article 60, ainsi qu'une description des projets de recherche à l'égard desquels une ordonnance a été rendue au titre de l'article 61.

#### 2.1.5 Recours
(articles 65 à 72 de la Loi sur la sécurité numérique)

Les articles 65 à 67 de la loi régissent la présentation d'observations du public à la Commission relativement à du contenu ou des comportements préjudiciables ou aux mesures prises par un exploitant pour se conformer à la loi. Aux termes de l'article 65, ces observations peuvent porter sur un contenu préjudiciable, un comportement préjudiciable auquel s'est livré un service d'agent conversationnel réglementé ou la façon dont l'exploitant d'un service réglementé s'acquitte des obligations qui lui incombent au titre de la présente loi. Ces observations peuvent être communiquées à l'exploitant ou rendues publiques (paragraphes 65(2) et 65(3)). Les articles 66 et 67 prévoient les exigences de confidentialité associées à ces observations.

Les articles 68 à 72 de la loi établissent les procédures de dépôt et de traitement des plaintes à la Commission portant sur du contenu « représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants ou du contenu intime communiqué de façon non consensuelle ». Aux termes de l'article 68, ce recours n'est possible qu'après avoir épuisé ceux prévus aux articles 44 et 46, et la Commission peut soit rejeter la plainte, soit ordonner que le contenu soit rendu inaccessible.

#### 2.1.6 Exécution et contrôle d'application
(articles 73 à 112 de la Loi sur la sécurité numérique)

Les articles 73 à 112 de la Loi sur la sécurité numérique énoncent les pouvoirs de la Commission en vue d'assurer le respect de la loi. Selon les règles qu'elle peut se donner en vertu de la Loi sur la Commission canadienne de la sécurité numérique, la Commission peut assigner des témoins à comparaître au même titre qu'une cour supérieure. Elle peut également faire prêter serment et trancher des questions de procédure ou de preuve. N'étant pas liée par les règles juridiques ou techniques applicables en matière de preuve, la Commission peut admettre des éléments de preuve qui ne seraient pas recevables dans une cour de justice. Elle a pour seule

VERSION PRÉLIMINAIRE
NON RÉVISÉE

obligation le devoir d'agir rapidement et sans formalité, en respectant les principes d'équité et de justice naturelle (articles 73 et 74).

La Commission peut tenir ses audiences de la manière qu'elle juge appropriée. Les audiences doivent être publiques, à moins que la Commission estime que le huis clos soit plus approprié après pondération de l'intérêt public et des considérations en matière de vie privée et de confidentialité (articles 75 et 76).

La Commission peut désigner un inspecteur pour vérifier le respect de la loi (article 77). L'inspecteur peut entrer dans tout lieu, physiquement ou par un moyen électronique, avec ou sans le consentement de l'occupant, ou en vertu d'un mandat délivré par un juge de paix, afin de confirmer que la loi est respectée ou d'empêcher qu'elle soit violée. L'inspecteur ne peut employer la force, à moins d'y être expressément autorisé par mandat et d'être accompagné d'un agent de la paix (paragraphe 79(3)).

La Commission peut rendre une ordonnance de son propre chef ou par l'entremise de la Cour fédérale afin d'empêcher un exploitant de contrevenir à la loi (articles 81 et 82).

En cas de contravention à ses dispositions ou à ses règlements, la Loi sur la sécurité numérique prévoit deux procédures distinctes : un régime de sanctions administratives pécuniaires (SAP) et la procédure pénale.

La procédure pénale (articles 107 à 110) est plus restreinte que le régime de SAP, s'appliquant à l'exploitant qui contrevient à une ordonnance de la Commission, omet de se conformer à tout engagement contracté avec la Commission ou à toute obligation que lui impose la Commission, entrave l'action de la Commission ou fait une déclaration fausse ou trompeuse à la Commission.

Ces actes ou omissions peuvent aussi faire l'objet d'une procédure en violation au titre du régime de SAP, mais la procédure en violation et la procédure pénale s'excluent l'une l'autre (article 103). Les sanctions maximales (amendes), énoncées à l'article 107 dans le cas des exploitants et à l'article 108 dans le cas des personnes autres qu'un exploitant, varient selon que l'infraction est poursuivie par mise en accusation ou par procédure sommaire et qu'il s'agit d'un individu. Les amendes maximales consistent en la somme la plus élevée entre un montant déterminé et un pourcentage déterminé des revenus bruts globaux, lesquels seront calculés conformément aux mesures réglementaires qui seront établies en vertu de l'article 112. L'amende maximale la plus élevée prévue aux termes de ces articles est de 5 % des revenus bruts globaux ou de 20 millions de dollars, dans le cas d'un exploitant, autre qu'un individu, déclaré coupable par mise en accusation.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Une personne autre qu'un exploitant commet une infraction si elle omet d'aider l'inspecteur à exercer ses attributions ou de lui fournir les documents ou renseignements qu'il exige (section 108). La peine d'emprisonnement est exclue en cas de défaut de paiement d'une amende infligée en vertu de la loi (article 111).

Le régime de SAP (articles 83 à 106) s'applique, à l'égard de l'exploitant, à tout acte ou omission pouvant faire l'objet de la procédure pénale, en plus de s'appliquer plus généralement à toute disposition de la loi ou de ses règlements, et plus particulièrement à tout exploitant qui omet de fournir des renseignements ou qui entrave l'action d'un inspecteur.

Le régime s'applique également à l'exploitant d'un service non réglementé (à savoir que la personne n'est pas visée par la définition du terme « exploitant ») s'il omet de se conformer à l'obligation de fournir des renseignements, omet de se conformer à toute obligation que lui impose un inspecteur, entrave l'action de la Commission ou fait une déclaration fausse ou trompeuse à la Commission (paragraphe 83(2)). Un service n'est pas considéré comme un « service réglementé » s'il n'atteint pas le seuil d'utilisateurs fixé à l'article 6 et qu'il n'est pas visé par règlement.

Les sanctions maximales sont établies à l'article 88. L'article 89 énonce les critères à prendre en compte pour la détermination de la sanction, bien que des critères supplémentaires puissent être établis en vertu de l'alinéa 112c). Une violation distincte est comptée pour chacun des jours au cours desquels se commet où se continue la violation (article 84).

L'article 85 précise que les sanctions imposées en vertu de ce régime ne visent pas à punir, mais à favoriser le respect de la loi. Les articles 93 à 96 décrivent la procédure pour contracter un engagement avec la Commission à l'égard des actes ou omissions visées.

#### 2.1.7 Protections, rapports et échange de renseignements (articles 113 à 124 de la Loi sur la sécurité numérique)

Les articles 113 à 116 de la Loi sur la sécurité numérique prévoient des protections juridiques pour divers types de personnes et de renseignements. Par exemple, l'article 113 stipule que, dans certains cas, les personnes agissant au nom de la Commission n'ont pas qualité pour témoigner dans certains types de procédure judiciaire. L'article 114 de la loi donne aux personnes le pouvoir de désigner comme confidentiels certains types de renseignements présentés à la Commission, notamment les secrets industriels ainsi que les renseignements commerciaux ou techniques. La Commission ne peut communiquer ce type de renseignements que si leur communication est dans l'intérêt public (paragraphe 114(5)). L'article 115 de la loi crée une infraction punissable par voie de procédure sommaire pour la

VERSION PRÉLIMINAIRE
NON RÉVISÉE

communication de renseignements confidentiels, la sanction maximale prévue étant de 5 000 $ pour la première infraction.

Les articles 117 à 119 de la loi énoncent les détails relatifs aux rapports que présente la Commission au ministre[59], y compris les exigences ayant trait au contenu du rapport annuel et à la production de rapports supplémentaires à la demande du ministre.

La Commission peut travailler avec des ministères et organismes fédéraux aux fins de la mise en œuvre de la loi aux conditions établies à l'article 120. Aux termes des articles 121 à 123 de la loi, la Commission doit consulter le Conseil de la radiodiffusion et des télécommunications canadiennes, le Commissaire à la protection de la vie privée[60] et la GRC relativement à diverses responsabilités en vertu de la loi. L'article 124 autorise également la Commission à fournir au ministre ou à une personne désignée par ce dernier certains renseignements pour aider à la prise d'un règlement en vertu de la loi et pour veiller « à la mise à jour et à l'efficacité » de la loi et de ses règlements.

#### 2.1.8 Règlements
(articles 126 et 127 de la Loi sur la sécurité numérique)

Aux termes de l'article 126, la Commission a le pouvoir de prendre des règlements sur un large éventail de sujets relatifs à la loi. Le gouverneur en conseil a aussi le pouvoir de prendre des règlements concernant certains sujets énumérés à l'article 127.

#### 2.1.9 Examens par le ministre
(articles 128 et 129 de la Loi sur la sécurité numérique)

L'article 128 de la loi prévoit un examen de l'ensemble de la loi par le ministre au troisième anniversaire de l'entrée en vigueur du présent article et tous les cinq ans par la suite. Le rapport doit être déposé au Sénat et à la Chambre des communes.

L'article 129 de la loi prévoit un examen des articles 27 à 29 au troisième anniversaire de l'entrée en vigueur du présent article. Les articles 27 à 29 portent sur l'obligation imposée aux exploitants de mettre en œuvre des mesures pour veiller à ce que les utilisateurs d'un service de média social réglementé aient l'âge minimal requis pour avoir un compte.

#### 2.1.10 Entrée en vigueur
(article 130 de la Loi sur la sécurité numérique)

Aux termes de l'article 130 de la loi, la loi entrera en vigueur à la date ou aux dates fixées par décret.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

#### 2.1.11 Disposition de coordination (article 3 du projet de loi C-34)

L'article 3 de la partie 1 du projet de loi C-34 coordonne le texte de plusieurs dispositions de la loi dans l'éventualité où le projet de loi C-16, Loi modifiant certaines lois en matière pénale et correctionnelle (protection de l'enfance, violence fondée sur le sexe, délais et autres mesures) recevrait la sanction royale avant le projet de loi C-34. Le 18 juin 2026, le projet de loi C-16 a reçu la sanction royale.

### 2.2 PARTIE 2 : LOI SUR LA COMMISSION CANADIENNE DE LA SÉCURITÉ NUMÉRIQUE

L'article 4 de la partie 2 du projet de loi C-34 édicte la Loi constituant la Commission canadienne de la sécurité numérique (titre subsidiaire : Loi sur la Commission canadienne de la sécurité numérique)[61]. La Commission est composée de trois à cinq membres à temps plein[62] nommés par le gouverneur en conseil (article 10), y compris le président (article 17), pour des mandats renouvelables d'au plus cinq ans (article 11). À titre de disposition transitoire, le président, une fois désigné, peut exercer tous les pouvoirs conférés à la Commission jusqu'à ce qu'au moins deux autres membres soient en fonction (article 23).

Dans des circonstances exceptionnelles, comme en cas d'allégations de faute grave ou en cas de risque pour la sécurité des employés, le gouverneur en conseil peut suspendre un membre de la Commission, avec traitement, jusqu'à ce qu'il ait déterminé si le membre devrait être destitué (article 14).

Le mandat de la Commission est d'exercer les attributions que lui confère la Loi sur la sécurité numérique ou toute autre loi fédérale (article 6). Comme mentionné ci-dessus, ces attributions comprennent la promotion de la sécurité en ligne au Canada, la réduction des préjudices causés par certains contenus en ligne, la prise de règlements et l'établissement de lignes directrices et de codes de conduite pour les services réglementés[63].

Dans les trois mois suivant la fin de chaque exercice, la Commission doit présenter au ministre un rapport sur les activités qu'elle a exercées au cours de cet exercice. Le ministre dispose alors de quinze jours de séance pour déposer le rapport devant chaque chambre du Parlement (article 21).

La Loi sur la Commission canadienne de la sécurité numérique entre en vigueur à la date ou aux dates fixées par décret (article 24).

Les articles 5 à 10 du projet de loi ajoutent la Commission canadienne de la sécurité numérique à certaines listes d'institutions fédérales dans la *Loi sur l'accès à l'information*, la *Loi sur la gestion des finances publiques*, la *Loi sur la protection des renseignements personnels* et la *Loi sur la pension de la fonction publique*.

---

NOTES

1. Projet de loi C-34, Loi édictant la Loi sur la sécurité numérique et la Loi sur la Commission canadienne de la sécurité numérique et apportant des modifications corrélatives à d'autres lois, 45e législature, 1re session.
2. Voir Projet de loi C-36, Loi édictant la Loi visant à protéger la vie privée et les données des consommateurs, modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et apportant des modifications à d'autres lois, 45e législature, 1re session; et Alexandra Savoie et Maxime-Olivier Thibodeau, *Résumé législatif du projet de loi C-36 : Loi édictant la Loi visant à protéger la vie privée et les données des consommateurs, modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et apportant des modifications à d'autres lois*, version préliminaire (non révisée), Bibliothèque du Parlement, 6 juillet 2026.
3. Anatoliy Gruzd et Philip Mai, *The State of Social Media in Canada 2025: A Census-balanced Survey About Social Media Adoption in Canada*, Social Media Lab, Toronto Metropolitan University.
4. Statistique Canada, « La haine et l'agression en ligne chez les jeunes au Canada », *Le Quotidien*, 27 février 2024.
5. Laura Savage, « L'exploitation sexuelle des enfants en ligne : un profil statistique des affaires déclarées par la police au Canada, 2024 », *Juristat*, Statistique Canada, 10 mars 2026. Notons que cyberaide.ca, la centrale canadienne de signalement des cas d'exploitation et d'abus sexuels d'enfants en ligne, a reçu 28 453 signalements du public en 2024-2025. Voir Sécurité publique Canada, *À propos de l'exploitation sexuelle des enfants en ligne*.
6. Statistique Canada, « Statistiques sur les crimes déclarés par la police au Canada, 2024 (tableau 5) », *Le Quotidien*, 22 juillet 2025.
7. Laura Savage, « L'exploitation sexuelle des enfants en ligne : un profil statistique des affaires déclarées par la police au Canada, 2024 », *Juristat*, Statistique Canada, 10 mars 2026.
8. *Ibid*.
9. Statistique Canada, *Les activités en ligne des jeunes Canadiens, la cybervictimisation et l'exposition à du contenu préjudiciable*, 23 avril 2025.
10. *Ibid*.
11. Femmes et Égalité des genres Canada, *Document infographique : Violence en ligne*.
12. Adam Cotter et Marta Burczycka, « Différences entre les genres observées dans les expériences de violence et de comportements sexuels non désirés au Canada, 2025 », *Juristat*, Statistique Canada, 31 mars 2026.
13. *Ibid*.
14. Femmes et Égalité des genres Canada, *Qu'est-ce que l'androsphère : termes clés, significations et importance*.
15. American Psychological Association, *Health advisory on social media use in adolescence*, mai 2023. Voir aussi États-Unis, Office of the Surgeon General, « Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory », *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, 2023.
16. Anatoliy Gruzd, Philip Mai et Anthony Clements Haines, *[New Report] The State of Generative AI Use in Canada 2025: Exploring Public Attitudes and Adoption Trends*, Social Media Lab, Toronto Metropolitan University, 8 avril 2025.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

17. UNICEF, *When AI becomes a friend: Child rights risks, harms, and regulatory responses to AI chatbots and companions*, exposé de politique, juin 2026, p. 3.

18. Royaume-Uni, *Online Safety Act 2023*, 2023, ch. 50.

19. Union européenne, EUR-Lex, *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)*, dans *Journal officiel*, nº L 277.

20. Australie, *Enhancing Online Safety Act 2015* (nº 24, 2015); Australie, *Online Safety Act 2021* (nº 76, 2011); et Australie, *Online Safety Amendment (Social Media Minimum Age) Act 2024* (nº 127, 2024).

21. Voir, par exemple, Union européenne, EUR-Lex, *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*, dans *Journal officiel*, série L; et l'annexe 5 et l'annexe 6 de la *Online Safety Act 2021* de l'Australie.

22 La notion de la responsabilité des plateformes, ou « responsabilité des intermédiaires d'Internet », est au cœur des débats sur les préjudices en ligne; on se demande si l'on peut considérer les plateformes comme des « éditeurs », étant donné qu'elles misent sur les algorithmes pour promouvoir leur contenu auprès des utilisateurs. Certaines personnes ont avancé qu'on peut considérer les plateformes comme des éditeurs, car le degré de sophistication de ces algorithmes leur permet de savoir qu'un contenu est préjudiciable avant de le publier. Voir, par exemple, l'analyse présentée dans : Friends of Canadian Broadcasting, *Platform for harm: Internet intermediary liability in Canadian law*, septembre 2020. Voir aussi *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, par. 89, 98, 99, 101 et 127 (dans le contexte de la *Loi sur le droit d'auteur*). Des conseils scolaires ont récemment intenté des poursuites contre des exploitants de médias sociaux (Caroline Alphonso, « Four Ontario school boards sue Instagram, Snapchat, TikTok owners over platforms' alleged harm to students », *The Globe and Mail*, 28 mars 2024 [ABONNEMENT REQUIS]).

23. *Code criminel*, L.R.C. 1985, ch. C-46.

24 En fait, on a modifié le *Code criminel* en 2014 pour préciser qu'en ce qui concerne une infraction comportant un élément de communication, la communication peut se faire par tout moyen de télécommunication (ce qui comprend Internet) (par. 4(8)).

25. *Loi visant à lutter contre la haine*, L.C. 2026, ch. 15.

26. Lors de sa comparution devant le Comité permanent de la justice et des droits de la personne de la Chambre des communes sur le Projet de loi C-9, Loi visant à lutter contre la haine, le ministre de la Justice et procureur général du Canada, l'honorable Sean Fraser, a confirmé que cette loi s'appliquerait également à Internet. Voir Comité permanent de la justice et des droits de la personne de la Chambre des communes, *Témoignages*, 9 octobre 2025.

27. À cet égard, voir l'article 320.1 du *Code criminel*.

28. *Loi sur la protection des Canadiens contre la cybercriminalité*, L.C. 2014, ch. 31.

29. *Loi visant à protéger les victimes*, L.C. 2026, ch. 19.

30. Bureau du premier ministre, le très hon. Justin Trudeau, C.P., *Lettre de mandat du ministre du Patrimoine canadien*, 13 décembre 2019; Bureau du premier ministre, le très hon. Justin Trudeau, C.P., *Lettre de mandat du ministre de la Justice et procureur général du Canada*, 13 décembre 2019; Bureau du premier ministre, le très hon. Justin Trudeau, C.P., *Lettre de mandat du ministre du Patrimoine canadien*, 16 décembre 2021; Bureau du premier ministre, le très hon. Justin Trudeau, C.P., *Lettre de mandat supplémentaire du ministre de la Justice et procureur général du Canada*, 15 janvier 2021.

31. Gouvernement du Canada, *Discours du Trône*, 23 septembre 2020.

32. Patrimoine canadien, *Document technique*.

33. *Loi concernant la déclaration obligatoire de matériel d'abus et d'exploitation pédosexuels sur Internet par les personnes qui fournissent des services Internet*, L.C. 2011, ch. 4.

34. Patrimoine canadien, *Résumé de l'atelier de clôture*.

35. Patrimoine canadien, *Ce que nous avons entendu : tables rondes sur la sécurité en ligne 2022*.

36. Troisième Assemblée citoyenne canadienne sur l'expression démocratique, *Assemblée citoyenne canadienne sur l'expression démocratique : Recommandations pour réduire les préjudices en ligne et protéger les droits de la personne au Canada*, Forum des politiques publiques, septembre 2022.

37. Projet de loi C-63, Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois, 44e législature, 1re session.

38. Chambre des communes, Comité permanent de la justice et des droits de la personne, *Objet du projet de loi C-63, Loi édictant la Loi sur les préjudices en ligne, modifiant le Code criminel, la Loi canadienne sur les droits de la personne et la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet et apportant des modifications corrélatives et connexes à d'autres lois*, 44e législature, 1re session.

39. Patrimoine canadien, *Le gouvernement du Canada convoque à nouveau le groupe consultatif d'experts sur la sécurité en ligne*, communiqué, 12 mars 2026.

40. Chambre des communes, Comité permanent de la justice et des droits de la personne, *Agir pour mettre fin à la haine en ligne*, vingt-neuvième rapport, juin 2019.

41. Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Assurer la protection de la vie privée et de la réputation sur les plateformes comme Pornhub*, troisième rapport, juin 2021.

42. Chambre des communes, Comité permanent de la sécurité publique et nationale, *La montée de l'extrémisme violent à caractère idéologique au Canada*, sixième rapport, juin 2022.

43. Sénat, Comité permanent des droits de la personne, *Combattre la haine : l'islamophobie et ses répercussions sur les musulmans au Canada*, novembre 2023.

44. Chambre des communes, Comité permanent de la justice et des droits de la personne, *La montée de l'islamophobie : Agir, faire face à la haine et protéger les libertés civiles ensemble*, vingt-sixième rapport, décembre 2024.

45. Chambre des communes, Comité permanent de la justice et des droits de la personne, *La montée de l'antisémitisme au Canada et les moyens d'y faire face*, vingt-septième rapport, décembre 2024.

46. Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Encadrement des plateformes de médias sociaux : Assurer la protection de la vie privée et la sécurité en ligne*, seizième rapport, décembre 2024.

47. Chambre des communes, Comité permanent du patrimoine canadien, *Torts causés par le matériel sexuellement explicite illégal en ligne*, quatorzième rapport, novembre 2024.

48. Chambre des communes, Comité permanent de la condition féminine, *La lutte contre les idéologies antiféministes au Canada*, sixième rapport, juin 2026.

49. Chambre des communes, Comité permanent du patrimoine canadien, *Les effets des influenceurs et des contenus des réseaux sociaux sur les enfants et les adolescents*, huitième rapport, juin 2026.

50. Sénat, Comité permanent des droits de la personne, *Solidaires et unis contre l'antisémitisme : Protéger les communautés et renforcer la démocratie canadienne*, avril 2026.

51. Sénat, Comité permanent des affaires sociales, des sciences et de la technologie, *Alimentée par la technologie, animée par l'humanité : Rapport provisoire sur une approche de l'IA centrée sur l'humain au Canada*, June 2026.

52. Projet de loi S-210, Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite, 44e législature, 1re session. Un projet de loi essentiellement semblable avait été présenté au cours de la 2e session de la 43e législature : projet de loi S-203, Loi limitant l'accès en ligne des jeunes au matériel sexuellement explicite.

53. Projet de loi S-209, Loi limitant l'accès en ligne des jeunes au matériel pornographique, 45e législature, 1re session; Pour obtenir plus de renseignements, voir : Dana Phillips, *Résumé législatif du projet de loi S-209 : Loi limitant l'accès en ligne des jeunes au matériel pornographique*, version préliminaire (non révisée), Bibliothèque du Parlement, 21 mai 2026.

54. L'article 17 du projet de loi C-36 ajouterait, à l'égard du droit à la protection de la vie privée, à l'article 18, « et, dans la mesure qu'elle l'estime indiquée, l'objet de la *Loi visant à protéger la vie privée et les données des consommateurs* ».

55. Il convient de noter que les intervenants ont soulevé des préoccupations en matière de protection de la vie privée et d'égalité de l'accès à l'égard des mesures de vérification et d'estimation de l'âge. Dans *Contrôle de l'âge – Note de politique* (2026), le Commissariat à la protection de la vie privée du Canada mentionne que le contrôle de l'âge peut nécessiter la collecte et le traitement de pièces d'identité, d'images faciales et d'autres renseignements personnels, pouvant exposer les personnes à des atteintes à la sécurité des données et à des activités de profilage et de surveillance dont les effets pourraient être disproportionnés pour certains groupes. Le Commissariat à la protection de la vie privée mentionne aussi, dans *Concevoir des systèmes de contrôle de l'âge qui protègent la vie privée – Document d'orientation pour les développeurs de systèmes de contrôle de l'âge*, que les systèmes d'estimation de l'âge en fonction du visage peuvent être moins précis selon la couleur de la peau et l'identité de genre, et que les méthodes de vérifications fondées sur des documents délivrés par un gouvernement peuvent ne pas reconnaître les pièces d'identité délivrées par les gouvernements autochtones et peuvent aussi avoir des répercussions indues sur des groupes comme les personnes itinérantes, les nouveaux arrivants et les personnes qui utilisent des appareils partagés ou publics.

    On a également mentionné que les limites d'âge pour les médias sociaux pourraient susciter des préoccupations en matière d'expression. En France, le 14 août 2026, le Conseil constitutionnel a annulé une interdiction de médias sociaux pour les enfants de moins de 15 ans, déclarant que l'interdiction portait atteinte à la liberté d'expression et de communication pour les moins de 15 ans (France, Conseil constitutionnel, *Décision no. 2026-911 DC du 14 août 2026, Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux*, 14 août 2026). Une telle interdiction pourrait aussi avoir une incidence sur les jeunes qui comptent sur les espaces en ligne pour l'information, l'appartenance communautaire et le soutien : dans *Drawing a line in digital spaces: Age-based restriction of social media* (2025), l'UNICEF note que les restrictions en fonction de l'âge peuvent limiter l'accès à l'apprentissage et aux renseignements sur la santé et avoir une incidence sur les enfants en milieu rural et défavorisé et ceux qui sont les plus discriminés et qui comptent sur les médias sociaux pour trouver des ressources et des opportunités, tout en poussant les jeunes utilisateurs vers des espaces moins réglementés.

56. Selon ce que prévoit la réglementation (articles 42, 58 et 59).

57. Selon la définition du paragraphe 2(1) de la Loi sur la sécurité numérique, le terme « personne » : « Vise notamment les personnes morales ainsi que les fiducies, les sociétés de personnes, les fonds, les coentreprises ou toutes autres associations ou organisations non dotées de la personnalité morale. »

58. L'objet de la Loi sur la sécurité numérique, énoncé à l'article 14, comprend la promotion de la sécurité et la protection de la santé physique et mentale des enfants.

59. Le terme « ministre » est défini au paragraphe 2(1) de la Loi sur la sécurité numérique. S'entend du ministre « le membre du Conseil privé du Roi pour le Canada désigné en vertu de l'article 13 ou, à défaut de désignation, le ministre du Patrimoine canadien. »

60. L'article 18 du projet de loi C-36 abrogerait l'article 122 de la loi sur la sécurité numérique, lequel exige que la Commission et le Commissaire à la protection de la vie privée du Canada se consultent mutuellement. L'article 18 du projet de loi exige de la Commission qu'elle consulte le Commissaire à la protection de la vie privée avant de publier des lignes directrices, y compris celles concernant les mesures de vérification et d'estimation de l'âge, ou de prendre un règlement, et qu'elle tienne compte de ses recommandations.

61. Notons que les articles 8 et 9 du projet de loi C-36 modifieraient les titres long et subsidiaire de la Loi sur la Commission canadienne de la sécurité numérique en ajoutant « et de la protection des données » après les mots « sécurité numérique » et en chargeant la Commission de l'application de la Loi visant à protéger la vie privée et les données des consommateurs et de la Loi sur la sécurité numérique.

62. L'article 13 du projet de loi C-36 modifierait l'article 10 de la Loi sur la Commission canadienne de la sécurité numérique afin que la Commission soit composée de cinq membres à temps plein.

63. L'article 12 du projet de loi C-36 ajouterait le nouveau paragraphe 6(1.1), selon lequel la Commission exerce les attributions que lui confère la Loi visant à protéger la vie privée et les données des consommateurs.