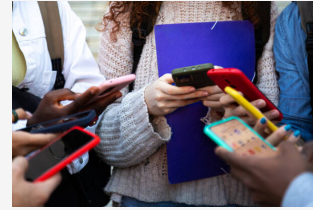


Le projet de loi C-34 en bref : la nouvelle Loi sur la sécurité numérique du Canada

25 JUIN 2026 18 MIN DE LECTURE



Expertises Connexes

- [Respect de la vie privée et gestion de l'information](#)
- [Technologie](#)

Auteurs(trice): [John Salloum](#), [Sam Ip](#), [Maryna Polataiko](#), [François Joli-Coeur](#), [Tina Saban](#)

Key Takeaways

- Le projet de loi C-34 promulguerait la nouvelle *Loi sur la sécurité numérique*, qui s'appliquerait à trois « services réglementés » : les médias sociaux, les agents conversationnels et les services en ligne.
- Les obligations communes à tous les exploitants comprennent notamment celles de protéger les enfants, d'agir de manière responsable et de faire preuve de transparence.
- Les mesures de protection des enfants comprendraient des caractéristiques de conception axées sur la sécurité et des restrictions en fonction de l'âge.
- Les exploitants de médias sociaux seraient tenus de supprimer, dans un délai de 24 heures, le matériel d'abus et d'exploitation pédosexuels (MAEP) et les images intimes distribuées de manière non consensuelle (IIDNC).
- La Loi serait l'un des premiers instruments législatifs canadiens à imposer des obligations directes en matière de sécurité aux exploitants de « services d'agents conversationnels » basés sur l'IA.
- Les sanctions administratives pécuniaires pourraient s'élever au plus à 3 % des revenus bruts globaux ou à 10 millions de dollars, selon le montant le plus élevé, et les infractions pourraient donner lieu à une amende pouvant s'élever au plus à 5 % des revenus bruts globaux ou à 20 millions de dollars, selon le montant le plus élevé.

Le gouvernement du Canada a mis en place un cadre juridique complet visant à encadrer la sécurité en ligne, à réduire les préjudices liés aux contenus en ligne et à instaurer des obligations de transparence et de responsabilité pour les exploitants de services réglementés, tels que les médias sociaux, les agents conversationnels et d'autres services en ligne. Le projet de loi C-34, intitulé « *Loi sur les médias sociaux sécuritaires* », crée deux nouvelles lois : la *Loi sur la sécurité numérique* (la « Loi »), qui impose des obligations aux exploitants de services réglementés, ainsi que la *Loi sur la Commission canadienne de la sécurité numérique*, qui institue l'organisme de réglementation chargé de l'exécution et du contrôle d'application de la Loi.

Réglementation des médias sociaux, des agents conversationnels et des services en ligne

Les obligations prévues par la Loi s'appliquent aux « services réglementés ». Un service est généralement considéré comme « réglementé » lorsqu'il correspond à un type de service défini, que son nombre d'utilisateurs atteint un seuil fixé par la réglementation ou qu'il est désigné comme un service réglementé par le gouverneur en conseil. Les obligations prévues par la Loi s'appliquent à trois types de « services réglementés » :

- **Les services de médias sociaux** : Les sites Web et les applications visant principalement à faciliter les communications entre les utilisateurs en leur permettant d'accéder à du contenu et de transmettre du contenu. Les services de médias sociaux comprennent les services de contenu pour adultes et les services de diffusion en direct. Les obligations prévues par la Loi ne s'appliquent pas aux fonctions de messagerie privée des services de médias sociaux.
- **Les services d'agents conversationnels** : Les systèmes d'intelligence artificielle (IA) qui i) communiquent par Internet, ii) sont accessibles par un site Web ou une application disponibles au public, iii) emploient une interface en langage naturel pour fournir, en mode conversationnel, des réponses qui sont adaptatives et qui pourraient avoir été formulées par un être humain, iv) peuvent simuler, par de multiples interactions ou lors de multiples séances, des relations durables semblables à celles que forment les êtres humains entre eux, et v) créent des contenus ou des réponses qui ne sont pas entièrement préconçus par le développeur ou l'exploitant du système. Les services d'agent conversationnel n'incluent pas les systèmes d'IA destinés exclusivement aux fins précisées dans la réglementation. Il convient de noter que la Loi ne semble pas contenir de définition distincte de l'expression « système d'intelligence artificielle ».
- **Les services en ligne** : Les sites Web ou les applications, autres que les services de médias sociaux ou les services d'agent conversationnel, qui permettent d'interagir avec eux. Les services en ligne n'incluent pas les sites Web ou les applications dont le but principal est de faciliter la vente, l'annonce ou la publicité de biens ou de services, ou de fournir un accès à des répertoires, des résultats de recherche, des cartes géographiques ou des outils de navigation. Les obligations prévues dans la Loi ne s'appliquent pas aux fonctions de messagerie privée des services en ligne. Pour être « réglementés », les services en ligne doivent appartenir à une « catégorie de services en ligne » qui, selon le gouverneur en conseil, présentent un risque important de préjudice pour les enfants au Canada.

Les fournisseurs de services de télécommunications qui assurent une connectivité de base à Internet seraient exemptés des obligations prévues dans la Loi. Aucune disposition de la Loi n'obligerait les exploitants à rechercher proactivement des contenus préjudiciables dans leurs services, mais la réglementation pourrait les obliger à utiliser des moyens technologiques pour empêcher le téléversement de matériel d'abus et d'exploitation pédosexuels (MAEP)^[1].

Étant donné que la Loi laisse le soin au gouvernement de préciser certains détails essentiels par règlement, le champ d'application exact de la Loi ne sera pas connu avant la publication

des projets de règlements.

Commission canadienne de la sécurité numérique

Le projet de loi C-34 prévoit la constitution de la Commission canadienne de la sécurité numérique. La Commission aurait pour mission de promouvoir la sécurité en ligne au Canada et de contribuer à réduire les préjudices causés à des personnes au Canada par du contenu préjudiciable en ligne, notamment en assurant l'exécution et le contrôle d'application de la Loi.

Contenus préjudiciables, pornographiques et synthétiques

La Loi viserait sept catégories de contenus préjudiciables : les images intimes distribuées de manière non consensuelle (IIDNC)^[2], le MAEP, 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 et le contenu de terrorisme ou d'extrémisme violent. La Loi instaurerait également des exigences particulières relativement aux contenus pornographiques et aux contenus synthétiques.

Obligations de base

La Loi imposerait deux obligations de base à tous les exploitants de services réglementés : 1) l'obligation de protéger les enfants, notamment grâce à des caractéristiques de conception axées sur la sécurité et à des mesures relatives à l'âge minimum requis pour avoir accès à du contenu pornographique, et (2) l'obligation de faire preuve de transparence par la tenue d'un registre de conformité.

L'obligation de protéger les enfants

- caractéristiques de conception axées sur la sécurité prévues par règlement;
- intégration de mesures de vérification ou d'estimation de l'âge jugées « adéquates » pour atténuer le risque que des enfants soient exposés à du contenu pornographique, lorsqu'un exploitant a des « motifs raisonnables » de soupçonner que son service donne accès à un tel contenu;
- toutes les mesures prévues par la réglementation pour réduire le risque que des enfants soient exposés à du contenu pornographique.

L'obligation de transparence

- tenue de registres nécessaires pour vérifier la conformité aux obligations prévues sous le régime de la Loi.

Obligations relatives aux médias sociaux

Pour les exploitants de services de médias sociaux réglementés, la Loi viendrait compléter ces deux obligations de base en ajoutant un régime d'âge minimum à l'obligation de protéger les enfants et des plans de sécurité numérique à l'obligation de transparence, et elle imposerait deux obligations supplémentaires, soit l'obligation d'agir de manière responsable en instaurant des mesures de sécurité intégrées aux systèmes et l'obligation de rendre les IIDNC et le MAEP inaccessibles.

L'obligation de protéger les enfants

- Si un service de médias sociaux réglementé est assujéti par voie réglementaire à des contraintes d'âge minimum, il doit intégrer des mesures « adéquates » de vérification ou d'estimation de l'âge « conçues pour empêcher » des personnes âgées de moins de 16 ans d'avoir un compte ou d'être inscrites auprès de ce service, ainsi que toutes autres mesures prévues par la réglementation.
- La Commission peut accorder une exemption à un exploitant qui prévoit dans le service en question des « mesures de protection adéquates » pour la protection des enfants.

L'obligation d'agir de manière responsable

- Mise en œuvre de mesures « adéquates » visant à atténuer le risque que les utilisateurs du service soient exposés à du contenu préjudiciable, et de toutes mesures visant à atténuer ce risque prescrites par règlement.
- Mise à la disposition des utilisateurs de lignes directrices qui définissent les normes de conduite qu'ils doivent respecter à l'égard du contenu préjudiciable et décrivent les mesures de conformité mises en œuvre par l'exploitant.
- Des outils qui permettent à des utilisateurs de bloquer d'autres utilisateurs et de signaler « facilement » les contenus préjudiciables, assortis d'obligations de notification pour les utilisateurs qui effectuent un signalement et les utilisateurs qui sont visés par un signalement.
- Des mesures « adéquates » visant à étiqueter le contenu synthétique qui répond aux critères prescrits lorsque cela est « raisonnable », ainsi que toute mesure prescrite concernant l'étiquetage de contenu synthétique.
- L'étiquetage de contenu préjudiciable dont l'exploitant a des « motifs raisonnables de croire » qu'il a été amplifié artificiellement par des programmes automatisés de tiers.
- Une personne-ressource « facile à trouver », dont les coordonnées sont « faciles d'accès », chargée de recueillir les préoccupations des utilisateurs, de les orienter vers des ressources internes et externes, et de les guider à l'égard des ressources internes.
- Le respect des exigences spécifiques de conservation et de destruction à la suite du retrait de contenu incitant à la violence, au terrorisme ou à l'extrémisme violent.

L'obligation de transparence

- La présentation à la Commission d'un plan de sécurité numérique comprenant des renseignements concernant :
 - la quantité et le type de contenu préjudiciable et le délai dans lequel il a été modéré, les signalements des utilisateurs, les caractéristiques de conception axées sur la sécurité des enfants et leur efficacité, les mesures relatives à l'âge minimum requis pour avoir accès à du contenu pornographique et les mesures relatives à l'âge minimum requis pour l'inscription des moins de 16 ans, les ressources allouées à la conformité, les recherches pertinentes et les mesures de déclaration obligatoire d'exploitation d'enfants, ainsi qu'un inventaire des données électroniques utilisées pour élaborer le plan;

- les critères et les processus, le cas échéant, régissant le signalement à la GRC ou à un autre organisme d'application de la loi de tout contenu qui laisse raisonnablement soupçonner qu'un individu risque de commettre un acte causant des lésions corporelles graves à un autre individu ou sa mort, avec des statistiques sur les signalements de ce type.
- La publication du plan de sécurité numérique dans un « format accessible et facile à consulter ».

L'obligation de rendre certains contenus inaccessibles

- L'obligation de retirer, dans les 24 heures, les IIDNC ou le MAEP qui sont repérés par les exploitants ou qui leur sont signalés, obligation qui va de pair avec les exigences d'application régulière de la loi (c.-à-d. les processus d'avis et d'appel).

Obligations relatives aux agents conversationnels

Pour les exploitants de services d'agents conversationnels réglementés, la Loi viendrait compléter l'obligation de base de transparence avec des plans de sécurité numérique et imposerait une obligation supplémentaire, soit celle d'agir de manière responsable, notamment en mettant en œuvre des mesures d'intervention en situation de crise et des mesures d'atténuation des risques liés à certains comportements préjudiciables.

L'obligation d'agir de manière responsable

- Des mesures « adéquates » visant à atténuer le risque de communication de contenu préjudiciable à un utilisateur, ainsi que toute mesure prescrite visant à atténuer ce risque
- Des mesures d'urgence prévoyant que, lorsqu'un utilisateur exprime des idées suicidaires, une intention de se mutiler ou une intention de commettre un acte qui pourrait causer des lésions corporelles graves à un individu, ou sa mort, le service interrompt immédiatement ses interactions avec l'utilisateur afin de l'orienter vers des services spécialisés en intervention de crise qui conviennent dans les circonstances, qui sont disponibles au moment où l'utilisateur est orienté vers ceux-ci et qui lui permettent d'interagir avec un être humain.
- Les mesures prescrites et les mesures « adéquates » visant à atténuer le risque que le service se livre à un comportement préjudiciable, et toutes autres mesures prescrites visant à atténuer le risque que le service se livre à un comportement préjudiciable, notamment un comportement consistant à :
 - se faire passer pour un être humain d'une manière qui pourrait porter l'utilisateur à croire qu'il s'agit d'un être humain ou dissimuler de toute autre manière le fait qu'il s'agit d'un système d'intelligence artificielle;
 - se faire passer pour un membre d'un ordre professionnel et donner, sur la base de cette tromperie, des conseils sur lesquels on pourrait raisonnablement s'attendre à ce que l'utilisateur se fie;
 - utiliser des « techniques d'engagement manipulatrices » pour maintenir un attachement émotionnel pouvant encourager l'utilisateur à se replier sur soi ou à perdre contact avec la réalité;

- encourager l'automutilation, le suicide ou la commission d'actes qui pourraient causer des lésions corporelles graves à un individu ou sa mort; et
- encourager tout autre comportement pros crit par règlement.
- Mettre à la disposition du public, des lignes directrices à l'intention des utilisateurs qui sont accessibles et faciles d'utilisation et prévoient notamment une description des mesures pour atténuer le risque de communication de contenu préjudiciable, des mesures pour répondre aux situations d'urgence et des mesures pour atténuer le risque que le service se livre aux comportements préjudiciables
- Mettre en œuvre des outils et des processus permettant aux utilisateurs de signaler facilement la communication d'un contenu préjudiciable, le défaut de répondre à une situation d'urgence ou le fait de s'être livré à un comportement préjudiciable, et d'être avisé de la réception de ce signalement
- Donner accès à une personne-ressource facile à trouver, dont les coordonnées sont faciles d'accès, qui est chargée de recevoir les préoccupations des utilisateurs à l'égard de la communication de contenu préjudiciable, de les orienter vers des ressources internes et externes et de les guider à l'égard de ces ressources internes.

L'obligation de transparence

- La remise à la Commission d'un plan de sécurité numérique comprenant :
 - des évaluations des risques de communication de contenu préjudiciable et du risque lié à des comportements préjudiciables, une description des mesures d'atténuation et une évaluation de leur efficacité, des renseignements concernant la quantité et le type de signalements des utilisateurs ainsi que les mesures qui en découlent, les caractéristiques de conception sur la sécurité des enfants et leur efficacité, les mesures relatives à l'âge minimum requis pour avoir accès à du contenu pornographique, les ressources allouées à la conformité, les recherches pertinentes et les mesures de signalement obligatoire d'exploitation d'enfant, ainsi qu'un inventaire des données électroniques utilisées pour élaborer le plan;
 - les critères et les processus, le cas échéant, régissant le signalement à la GRC ou à un autre organisme d'application de la loi de tout contenu qui laisse raisonnablement soupçonner qu'un individu risque de commettre un acte causant des lésions corporelles graves à un autre individu ou sa mort, avec des statistiques sur les signalements de ce type.
- La publication du plan de sécurité numérique dans un « format accessible et facile à consulter ».

Obligations relatives aux services en ligne

Pour les exploitants de services en ligne réglementés, la Loi complète l'obligation de transparence de base en y ajoutant l'obligation de présenter des plans de sécurité numérique.

L'obligation de transparence

- La présentation à la Commission d'un plan de sécurité numérique comprenant des renseignements sur ce qui suit :
 - les caractéristiques de conception axées sur la protection des mineurs et leur efficacité, les mesures relatives à l'âge minimum requis pour avoir accès à du contenu pornographique, les ressources allouées à la conformité (y compris pour la prise de décision automatisée), ainsi que les mesures de signalement obligatoire d'exploitation de mineurs, accompagnés d'un inventaire des données électroniques utilisées pour élaborer le plan;
 - les critères et les processus, le cas échéant, régissant le signalement à la GRC ou à un autre organisme d'application de la loi de tout contenu qui laisse raisonnablement soupçonner qu'un individu risque de commettre un acte causant des lésions corporelles graves à un autre individu ou sa mort, avec des statistiques sur les signalements de ce type.
- La publication du plan de sécurité numérique dans un « format accessible et facile à consulter ».

Accès aux inventaires et aux données électroniques

La Loi instaurerait un régime d'accès aux fins de recherches et habiliterait la Commission à : accréditer des personnes qui ont pour objectif principal d'effectuer des recherches ou de se livrer à des activités en matière d'éducation qui sont liées à l'objet de la présente loi; à leur permettre d'accéder aux inventaires de données électroniques inclus dans les plans de sécurité numérique de l'exploitant; et à rendre une ordonnance enjoignant à l'exploitant de donner, aux individus mentionnés dans la demande, l'accès aux données électroniques aux fins de projets de recherches. La Commission peut publier une liste des personnes accréditées et une description du projet de recherche à l'égard duquel elle a rendu cette ordonnance. La Commission pourrait publier une liste des personnes accréditées et une description des projets de recherche pour lesquels elle a prononcé des ordonnances d'accès.

Recours

La Loi permettrait à toute personne au Canada :

- de fournir à la Commission des observations à propos d'un contenu préjudiciable qui est accessible sur un service réglementé, d'un comportement préjudiciable d'un service d'agent conversationnel réglementé ou de la conformité d'un exploitant à la Loi;
- de déposer une plainte auprès de la Commission pour signaler que du contenu accessible sur un service de média social réglementé constitue des IIDNC ou du MAEP, et demander une ordonnance de retrait.

Exécution et contrôle d'application

Sous le régime de la Loi, la Commission disposerait de pouvoirs de contrôle d'application étendus, notamment pour faire ce qui suit :

- Procéder à l'examen des plaintes, y compris assigner et contraindre des témoins à comparaître devant elle, à déposer sous la foi du serment et à produire des documents, et

recevoir les éléments de preuve qu'elle estime indiqués, indépendamment de leur admissibilité devant les tribunaux;

- Tenir des audiences concernant les plaintes relatives à des IIDNC ou du MAEP, ainsi que toute autre question se rapportant au respect de la Loi par un exploitant;
- Entrer dans tout lieu à toute fin liée à la vérification du respect ou à la prévention du non-respect de la Loi, à condition d'être munie du mandat prévu par la Loi;
- Prononcer des ordonnances de conformité afin de contraindre un exploitant à prendre ou s'abstenir de prendre toute mesure pour assurer l'observation de la Loi, si la Commission a des motifs raisonnables de croire qu'un exploitant contrevient ou a contrevenu à la Loi.

Sous le régime de la Loi, les ordonnances de la Commission pourraient être homologuées par la Cour fédérale.

Sanctions administratives pécuniaires et infractions

La Loi instaurerait également de lourdes pénalités pour les exploitants qui l'enfreignent (à moins qu'ils n'invoquent une défense fondée sur les précautions voulues) :

- Des sanctions administratives pécuniaires pouvant atteindre au plus 3 % des revenus bruts globaux ou 10 millions de dollars, selon le plus élevé des deux montants, peuvent être imposées en cas de contravention à toute disposition de la Loi ou de ses règlements ou de non-respect de toute ordonnance de la Commission;
- Des amendes pouvant atteindre 5 % des revenus bruts globaux ou 20 millions de dollars, selon le plus élevé des deux montants, sur déclaration de culpabilité par mise en accusation, ou 4 % des revenus bruts globaux ou 15 millions de dollars, selon le plus élevé des deux montants, sur déclaration de culpabilité par procédure sommaire, ou pour une infraction telle que la violation d'une ordonnance de la Commission ou d'un engagement, l'entrave au travail d'un inspecteur ou la formulation de déclarations fausses ou trompeuses.

Lorsqu'un exploitant et d'autres personnes font partie d'un même groupe, l'expression « revenus bruts globaux » désigne les revenus bruts globaux du groupe. La Commission pourrait également publier des procès-verbaux et des engagements avec le nom des parties visées, et exiger des parties visées qu'elles publient elles-mêmes l'avis.

Série d'Osler sur les préjudices en ligne Le présent bulletin d'actualités est le quatrième volet de la série d'Osler sur les préjudices en ligne. Cette série suit l'évolution du cadre canadien en matière de sécurité en ligne, de réglementation des plateformes et de protection des renseignements personnels des enfants. Consultez les articles précédents : [Projet de loi C-16 : mises à jour du régime fédéral canadien de déclaration du matériel d'abus et d'exploitation pédosexuels](#) (18 décembre 2025) et [La nouvelle Loi sur les préjudices en ligne \(C-63\) du Canada : ce qu'il faut savoir](#) (1^{er} mars 2024).

^[1] La Loi utilise l'expression « contenu représentant de la victimisation sexuelle d'enfants ou perpétuant la victimisation de survivants », communément appelée matériel d'abus et

d'exploitation pédosexuels (MAEP).

^[2] La Loi utilise l'expression « contenu intime communiqué de façon non consensuelle », communément appelée « images intimes distribuées de manière non consensuelle » (IIDNC).