Combler les lacunes : **Lutter contre les images intimes non consensuelles facilitées par l 'IA au Canada et au Mexique.** Un diagnostic comparatif.

Auteures : **Daniela Rojas et Claudia Del Pozo**
Contributrices : **Nicté Cabañas et Amélie Côté**

Octobre 2026



IVADO

EON INSTITUTE

avec le soutien de

CANADA FIRST RESEARCH EXCELLENCE FUND

APOGÉE CANADA FONDS D'EXCELLENCE EN RECHERCHE

Remerciements

Les auteures souhaitent remercier toutes les personnes qui ont contribué à ce projet en participant à des entretiens dans les deux pays. Nous sommes extrêmement reconnaissantes du temps qu'elles nous ont accordé et des points de vue qu'elles ont partagés. Ces derniers ont façonné ce document d'information. Le nom de ces personnes est indiqué ci-dessous en ordre alphabétique.

Elizabeth Avendaño, avocate et activiste féministe, Luchadoras

Sénateur Luis Donaldo Colosio, président, Commission des droits numériques, Sénat du Mexique

Sarah Crawford, directrice générale, Centre canadien de ressources pour les victimes de crimes

Élise Dupras, spécialiste en délinquance et conseillère en cyberenjeux en milieu scolaire, Centre de services scolaire Marguerite-Bourgeoys

Marcela Hernández, cofondatrice, Defensoras Digitales

Floretta Mayerson, cofondatrice, Violetta

Paola Ricaurte Quijano, professeure-chercheuse, Tecnológico de Monterrey

Catherine Régis, professeure de droit, Université de Montréal

Teresa Scassa, professeure-chercheuse, Université d'Ottawa

Les propos exprimés dans le présent rapport ne reflètent pas nécessairement les points de vue des expertes et de l'expert consultés, mais demeurent ceux des autrices du rapport.

La préparation de ce document a été rendue possible grâce à une collaboration entre l'Eon Institute au Mexique et IVADO au Canada. Eon Institute est un think tank mexicain qui œuvre en Amérique latine pour renforcer la résilience des sociétés à l'ère de l'IA à travers la recherche appliquée, le renforcement des capacités et la mise en réseau, en reliant connaissances et acteurs afin de développer de meilleures politiques et stratégies. IVADO est un consortium de recherche et de mobilisation des connaissances intersectoriel et multidisciplinaire dirigé par l'Université de Montréal dont la mission est de concevoir et de promouvoir une IA robuste, raisonnante et responsable.

CONTENU

03 **Principaux points à retenir**

04 **Introduction**

05 **Impacts des images intimes non consensuelles facilitées par l'IA sur les individus et la société**

05 **Rôle des entreprises de technologies dans la chaîne de préjudices des images intimes non consensuelles facilitées par l'IA**

07 **Aperçu général des cadres réglementaires et des politiques publiques à l'échelle mondiale**

07 Tendances courantes dans la réglementation des images intimes non consensuelles

10 Tendances courantes dans la réglementation du matériel pédopornographique

10 États-Unis : la loi *TAKE IT DOWN* et au-delà

12 **Profil du pays : CANADA**

12 Aperçu de l'exploitation des images intimes non consensuelles au Canada

13 Cadre réglementaire

14 Mécanismes de dépôt de plaintes et de réparation

15 Lacunes en matière de réglementation, de mise en œuvre et de coordination

16 **Profil du pays : MEXIQUE**

16 Aperçu de l'exploitation des images intimes non consensuelles au Mexique

17 Cadre réglementaire

17 Mécanismes de dépôt de plaintes et de réparation

18 Lacunes en matière de réglementation, de mise en œuvre et de coordination

19 **Principaux constats comparatifs**

21 **Recommandations en matière de politiques publiques**

21 Recommandations de politiques transversales

23 Recommandations particulières pour le Canada

24 Recommandations particulières pour le Mexique

25 **Conclusion**

25 **Notes**

PRINCIPAUX POINTS À RETENIR

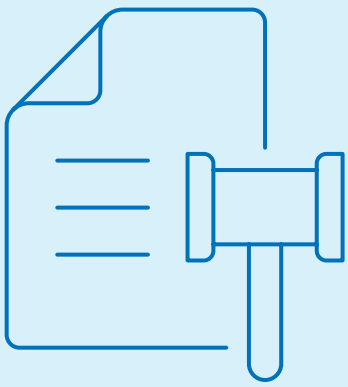
Ce rapport examine de quelle manière le Canada et le Mexique réagissent aux images intimes non consensuelles (IINC) facilitées par l'IA et identifie des lacunes structurelles dans les domaines de la prévention, de la réparation et de la responsabilité. Même si ces pays possèdent des traditions juridiques et des contextes institutionnels bien différents, ils font tous deux face aux mêmes défis sous-jacents.

Nos constats

- → Des cadres juridiques existent, mais ils ne se traduisent pas en justice. Au Mexique, seulement 0,5 % des plaintes liées aux IINC se rendent dans le système juridique. Au Canada, la protection civile varie considérablement selon la province de résidence des personnes survivantes, alors que les protections du *Code criminel* viennent d'être renforcées en juin 2026 et il faudra mieux étudier leur application.
- → La capacité des institutions est le principal écueil. Les procureures et procureurs, les juges et les membres des forces de l'ordre ne disposent pas de la formation technique ni de la perspective soucieuse des sexospécificités nécessaires pour enquêter efficacement et poursuivre en justice ces cas.
- → Les plateformes numériques exercent leurs activités sans obligations contraignantes. En juin 2026, le gouvernement du Canada a déposé le projet de loi C-34 afin de leur imposer de nouvelles obligations réglementaires. En octobre 2026, le Mexique a renforcé la protection des personnes mineures, sans préciser les modalités d'application ni prévoir de sanctions. De plus, la plupart des plateformes numériques se trouvent aux États-Unis et le chapitre sur le commerce numérique de l'Accord Canada–États-Unis–Mexique (ACEUM) limite la capacité des gouvernements canadien et mexicain d'exiger qu'elles répondent de leurs actions.
- → En raison des nombreuses barrières auxquelles elles font face, les personnes les plus touchées (les Autochtones, les femmes racialisées et les personnes mineures) sont celles qui ont le moins accès à la justice.

Nos recommandations

- → Pour les deux pays : coordonner une position commune lors de la révision prochaine de l'ACEUM afin d'établir des normes de responsabilité minimales pour les plateformes.
- → Pour le Canada : prioriser la mise en application des nouvelles mesures de la *Loi visant à protéger les victimes* (projet de loi C-16, adopté en juin 2026) ; prioriser l'adoption du projet de loi C-34 (*Loi sur les médias sociaux sécuritaires*), déposé en juin 2026 ; et élargir les mécanismes de réparation d'urgence à toutes les provinces.
- → Pour le Mexique : miser sur la mise en œuvre du cadre existant *Ley Olimpia* (Loi Olimpia) avant de créer d'autres lois et mettre en place des protocoles nationaux contraignants pour les procureures et procureurs, ainsi qu'un seul canal de signalement pour les personnes survivantes.



INTRODUCTION

La récente mise en œuvre à grande échelle des outils d'intelligence artificielle (IA) n'a pas simplement créé une violence fondée sur le sexe, elle l'a également fondamentalement transformée. L'IA générative a abaissé les barrières à la production et à la distribution d'images intimes non consensuelle (IINC) en nécessitant, de la part des personnes à leur origine, des compétences techniques et des coûts minimaux, et en réduisant leurs risques en matière de responsabilité. Au bout du compte, cette situation alimente une forme plus rapide et plus accessible de violence fondée sur le sexe facilitée par les technologies.

L'ampleur du phénomène est impressionnante. En date de 2023, 98 % des vidéos hypertruquées en ligne étaient non consensuelles, tandis que 99 % d'entre elles dépeignaient des femmes[1]. Le cas de Grok (le grand modèle de langage d'X) illustre bien ce phénomène : au début de 2026, il a été utilisé pour générer environ 1,8 million d'images à caractère sexuel de femmes en seulement neuf jours[2], ce qui correspond à deux images chaque seconde. La violence ne se limite pas aux adultes. Le même cas a également révélé des images d'abus pédosexuels impliquant de jeunes filles âgées de 11 à 13 ans[3]. En fait, les signalements d'images d'abus pédosexuels facilitées par l'IA (en anglais, l'acronyme CSAM est utilisé pour *child sexual abuse material*). ont augmenté de 1,325 % entre 2023 et 2024[4], une étude de cas menée en 2025 dans 11 pays révélant que les images d'au moins 1,2 million d'enfants ont été manipulées et intégrées à des hypertrucages sexuellement explicites[5]. En outre, l'Internet Watch Foundation (IWF) a répertorié 3 440 vidéos contenant des images d'abus pédosexuels facilitées par l'IA en 2025 comparativement à seulement 13 l'année précédente[6].

Malgré les preuves de plus en plus nombreuses des conséquences émotionnelles, économiques, sociales et démocratiques des IINC facilitées par l'IA, les mesures politiques mises en place restent inadéquates. En 2023, seul un tiers des économies disposait de lois protégeant les femmes contre le cyberharcèlement, notamment le Canada et le Mexique[7], et même lorsque de telles lois existent, les mécanismes d'application sont faibles.

Le Canada et le Mexique offrent un cadre comparatif particulièrement instructif. Les deux pays doivent composer avec les complexités de leur système fédéral respectif, tout en étant aux prises avec des plateformes numériques basées aux États-Unis qui échappent largement à leur champ de compétences réglementaires, sans compter leurs capacités limitées en matière d'application de la loi et le sous-financement de leurs systèmes de soutien aux personnes survivantes. Ce rapport examine de quelle manière le Canada et le Mexique réagissent aux IINC facilitées par l'IA, cerne les lacunes structurelles en matière de prévention, de réparation et de responsabilité dans les deux contextes, et formule des recommandations concrètes en matière de politiques à l'intention des décideuses et décideurs des deux pays.

Limites de la méthodologie

La méthodologie utilisée pour réaliser cette étude repose sur une approche qualitative, comparative et interdisciplinaire combinant une analyse de documents, notamment des cadres réglementaires, des ordonnances de la cour, des documents de la société civile et de la littérature universitaire, et neuf entretiens semi-structurés menés entre février et mars 2026 auprès d'expertes et d'experts issus de la société civile, du milieu universitaire, de la pratique juridique et des institutions publiques des deux pays. L'échantillon pour les entretiens a été sélectionné de manière ciblée, mais n'est pas exhaustif pour l'un ou l'autre des écosystèmes. Même si l'échantillon canadien ne comprend pas de représentante ou de représentant du pouvoir législatif, d'autres personnes interrogées se sont directement intéressées aux questions législatives par le biais de recherches, de contributions à des rapports officiels et de collaborations en matière de politiques publiques.

IMPACTS DES IMAGES INTIMES NON CONSENSUELLES FACILITÉES PAR L'IA SUR LES INDIVIDUS ET LA SOCIÉTÉ

Les espaces numériques sont devenus un terrain privilégié pour la violence fondée sur le sexe. Loin d'être de simples prolongements des préjudices subis dans la vie réelle, ils constituent des environnements dotés de leurs propres dynamiques, outils et structures de pouvoir, où des formes établies de violence trouvent de nouveaux moyens d'expression.

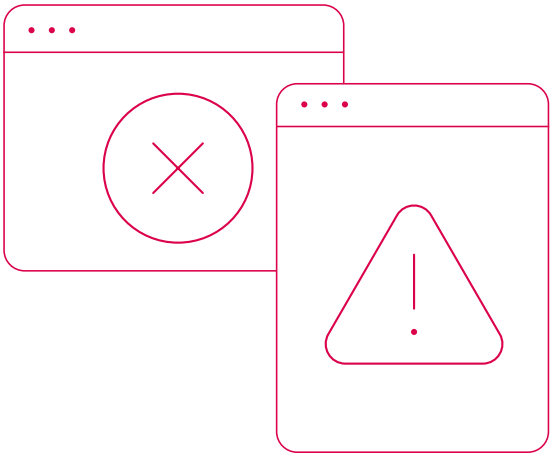
Une idée fausse courante façonnant les réponses des institutions est que la nature synthétique des IINC facilitées par l'IA causerait moins de préjudices. Les données suggèrent le contraire : les personnes survivantes souffrent de stress chronique, d'anxiété, de dépression et d'une érosion de l'estime de soi, et certaines d'entre elles se suicident[8], ce qui est comparable à ce que vivent les personnes survivantes d'IINC non synthétiques[9]. Ces conséquences s'étendent à la vie professionnelle et scolaire, portant atteinte à la réputation et perturbant l'assiduité, la concentration et le parcours scolaire[10]. Les personnes survivantes manquent souvent d'options juridiques ou techniques accessibles pour limiter les préjudices.

La dimension genrée de ce préjudice dépasse le cadre individuel et a des répercussions sociales plus larges. En tant que forme de contrôle social systématique, la normalisation des IINC facilitées par l'IA renforce l'objectivation des femmes, intensifie le harcèlement et dissuade la participation à la vie publique[11]. Lorsqu'il est utilisé contre des politiciennes, des journalistes, des militantes et des candidates, le contenu synthétique à caractère sexuel peut devenir un outil de violence politique, réduisant au silence les voix, sapant la crédibilité et décourageant l'engagement public[12]. Au Mexique, lors des élections de 2024, par exemple, 217 femmes ont retiré leur candidature en raison de pressions, de menaces ou de coercition, les plaintes officielles restant rares en raison de l'intimidation et d'une connaissance limitée des mécanismes de signalement[13].

Il est important de mentionner que ces préjudices ne sont pas des conséquences inévitables du progrès technologique. Ils sont la conséquence de choix de conceptions précis, de lacunes réglementaires, de limites institutionnelles et de responsabilité insuffisante de la part des entreprises de technologies.

RÔLE DES ENTREPRISES DE TECHNOLOGIES DANS LA CHAÎNE DE PRÉJUDICES DES IMAGES INTIMES NON CONSENSUELLES FACILITÉES PAR L'IA

Les préjudices que causent les IINC facilitées par l'IA découlent d'un écosystème interconnecté d'acteurs intervenant à différentes étapes de la chaîne de préjudices. Pour ce qui est de la création, il y a à la fois les applications de « nudification » alimentées par l'IA et les plateformes d'IA générative utilisées à mauvais escient, tandis que dans le cas de l'amplification, il y a les réseaux sociaux et les plateformes de contenu sur lesquels la violence se manifeste et est amplifiée. Le diagramme 1 illustre les différentes étapes de la chaîne de préjudices.



Chaîne de préjudices des IINC facilités par l'IA

Création

Applications de « nudification »

Explicitement conçues pour produire et stocker des IINC

Les grandes plateformes de pornographie profitent des IINC.

Marché ~ $117M ; ~ 705 M d'utilisateurs* en janvier 2026.

Infrastructure et services fournis par les plus grandes entreprises de technologie.

Plateformes d'IA générative

Non conçues pour être utilisées à mauvais escient, mais peuvent l'être

1,8 M d'images à caractère sexuel via Grok en 9 jours (2026).

Hausse de 1,325 % des signalements d'images d'abus pédosexuels facilitées par l'IA entre 2023 et 2024.

Incapacité des développeurs* de tester pour la mauvaise utilisation à des fins d'images d'abus pédosexuels.

Amplification

Plateformes de médias sociaux et de contenu

Où les préjudices se propagent, persistent et sont gouvernés

Détection automatisée des infractions en temps réel, avec un taux d'erreur pouvant atteindre 70 à 80 %.

Manque de transparence dans les rapports d'incidents et lenteur des réponses apportées aux personnes survivantes.

Accès limité pour le public aux données des entreprises.

*N.B. Dans le tableau, par souci de concision, nous avons utilisé que le masculin.

Pour ce qui est de la création, plusieurs plateformes, connues sous le nom d'applications de « nudification » alimentées par l'IA, sont conçues explicitement pour produire et héberger des IINC[14]. Ces applications sont devenues une affaire très lucrative, bien qu'il soit difficile de l'évaluer exactement. En janvier 2026, le Tech Transparency Project a évalué le marché à environ 117 millions de dollars américains et à 705 millions de téléchargements des applications de « nudification » avec l'IA. Plusieurs d'entre elles utilisant l'infrastructure et les services fournis par de grandes entreprises de technologies[15]. Deux grands fournisseurs de services infonuagiques fournissent l'infrastructure d'hébergement et de distribution de contenu à 62 des 85 sites de « nudification »[16]. Les plateformes d'IA générative s'avèrent aussi un défi, puisqu'elles peuvent être utilisées à mauvais escient pour créer des images intimes non consensuelles et des images d'abus pédosexuels, un risque que les développeuses et développeurs ne peuvent pas tester directement compte tenu de l'illégalité du traitement de ce type de contenu[17]. En réponse, le Royaume-Uni autorise un nombre limité d'organisations agréées à tester des modèles d'IA dans des conditions strictes[18].

Pour ce qui est de l'amplification, les plateformes de médias sociaux et de contenu établissent les règles gouvernant les comportements, la modération de contenu et l'application des règles. Même si plusieurs d'entre elles utilisent des systèmes d'IA pour détecter les infractions en temps réel, le problème n'est pas simplement l'inefficacité de la modération de contenu, qui peut atteindre des taux d'erreur de 70 à 80 %[19], mais bien le fait que les personnes chargées de la modération reçoivent des signalements ou des alertes sans disposer d'un contexte suffisant pour intervenir de manière appropriée[20]. De plus, les personnes survivantes signalent que l'intervention des plateformes est insuffisante, caractérisée par des temps de réponse trop longs, et qu'il y a un manque de transparence dans les processus de signalements et peu de suivis[21].

En outre, l'ampleur du problème est masquée par l'opacité systémique de ces plateformes qui contrôlent étroitement l'accès à l'information par le public, les chercheuses et chercheurs, les organisations de la société civile, et les décideuses et décideurs. Cela dit, certaines grandes entreprises

de réseaux sociaux ont commencé à reconnaître leur rôle, des plateformes comme Meta s'associant à des initiatives de la société civile telles que StopNCII.org[22] et *Take It Down*[23] pour faciliter le retrait des IINC. Elles ont également mis en place des politiques plus strictes interdisant à la fois les IINC traditionnelles et celles facilitées par l'IA[24].

Compte tenu de ces défis, un virage s'opère depuis quelques années : plutôt que de rejeter le blâme sur les individus qui partagent des IINC, on tend désormais à tenir les plateformes directement responsables. Les poursuites récentes sont, en fait, des signes de ce virage. Voici quelques exemples marquants : l'action judiciaire engagée par la France contre Telegram pour complicité dans des activités illégales, incluant la distribution d'images d'abus pédosexuels[25], la poursuite intentée par San Francisco (États-Unis) contre des sites Web créant des IINC hypertruquées facilitées avec l'IA[26], les poursuites engagées contre X par les autorités de Baltimore (États-Unis)[27], l'action judiciaire des Pays-Bas contre la facilitation et la distribution de masse d'IINC facilitées par l'IA par Grok[28], et le procès intenté contre Meta par le gouvernement du Nouveau-Mexique (États-Unis) pour avoir permis des préjudices, y compris l'exploitation sexuelle d'enfants, à l'encontre de ses utilisatrices et utilisateurs[29].

L'UE s'entend pour bannir les applications de « nudification » afin de protéger les citoyennes et citoyens

L'Union européenne est récemment parvenue à un accord politique visant à simplifier la mise en œuvre de la *Loi européenne sur l'intelligence artificielle* (la loi européenne complète sur l'IA), tout en renforçant les protections contre le contenu à caractère sexuel nuisible généré par l'IA. Cet accord interdit les systèmes d'IA qui créent des IINC (y compris les applications de « nudification ») ainsi que les images d'abus pédosexuels générées par l'IA. Les institutions de l'UE ont présenté ces modifications comme un effort visant à trouver un équilibre entre innovation, compétitivité et protection des droits fondamentaux[30].

APERÇU GÉNÉRAL DES CADRES RÉGLEMENTAIRES ET DES POLITIQUES PUBLIQUES À L'ÉCHELLE MONDIALE

Les images intimes non consensuelles facilitées par l'IA font partie d'une forme de préjudice qui fait l'objet de cadres politiques et juridiques depuis plus d'une décennie. Cependant, le fait de les avoir initialement qualifiées de « pornographie de vengeance » a réduit la portée du problème, occulté ses dimensions structurelles et genrées, et laissé des lacunes concernant le contenu synthétique et la responsabilité des plateformes.

Une brève analyse des tendances réglementaires mondiales relatives aux images intimes non consensuelles et aux images d'abus pédosexuels est fournie ci-dessous, ainsi qu'un aperçu du cadre juridique actuellement en place aux États-Unis, présenté en raison du rôle central que joue ce pays en tant que principale compétence pour la plupart des questions relatives à la gouvernance des plateformes.

Tendances courantes dans la réglementation des images intimes non consensuelles

Seulement 58 sur 190 pays ont adopté des lois visant à protéger les femmes contre le cyberharcèlement, protégeant, par le fait même, moins de la moitié de la population, et seules 7 économies prévoient des dommages-intérêts et/ou une indemnisation financière pour les personnes survivantes, en plus de sanctions pénales[31]. Pour ce qui est des IINC numériques, 117 pays rapportent, en date de 2025, avoir pris des mesures pour lutter contre elles[32]. Le tableau ci-dessous présente certaines lois adoptées à travers le monde pour lutter contre les IINC facilitées par l'IA.

Lois adoptées à travers le monde pour lutter contre les IINC facilitées par l'IA

Pays	Instrument juridique	Année	Portée de la criminalisation	Sanctions	Particularités
Australie	Projet de loi d'amendement au *Code criminel* (matériel hypertruqué à caractère sexuel)[33]	2024	Création et distribution d'IINC (y compris celles générées par l'IA)	Jusqu'à 7 ans d'emprisonnement.	• Accent mis sur la clarté juridique et l'harmonisation. • Le *Law Council* a mis en garde contre tout excès; le Sénat a appuyé le projet de loi, formulant des recommandations en matière de révision et d'harmonisation. • Première poursuite en vertu de la nouvelle infraction fédérale en 2026[34].
Canada	*Loi visant à protéger les victimes (*Projet de loi C-16, *Loi visant à protéger les victimes et à garder les enfants à l'abri des personnes prédatrices)*[35]	2026	La Loi élargit l'infraction interdisant la diffusion d'IINC afin de garantir qu'elle s'applique aux hypertrucages d'ordre sexuel non consensuels. Le *Code criminel* interdisait déjà la diffusion d'images intimes sans le consentement de la personne représentée, mais ne couvrait pas les menaces de diffusion de ces images, lesquelles sont un élément de plusieurs affaires d'extorsion d'ordre sexuel. La Loi interdit les menaces de diffusion d'images intimes, y compris des hypertrucages d'ordre sexuel, sans le consentement de la personne concernée. Les nouvelles infractions couvrent aussi les hypertrucages en lien avec le matériel d'abus et d'exploitation pédosexuels, ainsi que les représentations de bestialité.	Jusqu'à 7 ans d'emprisonnement.	• Augmentation de la peine maximale de 5 à 10 ans, lorsque l'infraction est poursuivie par mise en accusation pour la menace de distribuer sans le consentement de la personne représentée des images intimes, y compris des hypertrucages à caractère sexuel. • Ajout d'une circonstance aggravante à l'infraction d'extorsion au cas où cette infraction serait utilisée dans des affaires d'extorsion d'ordre sexuel. • Rétablissement des peines minimales obligatoires (PMO) qui avaient été jugées inopérantes par la Cour suprême du Canada, sauf lorsque la PMO entraînerait une peine manifestement disproportionnée.

Lois adoptées à travers le monde pour lutter contre les IINC facilitées par l'IA (suite)

Pays	Instrument juridique	Année	Portée de la criminalisation	Sanctions	Particularités
Danemark	*Loi danoise sur les droits d'auteur*[36]	2025	Utilisation non autorisée de l'image ou de la voix d'une personne, telles que protégées par le droit d'auteur	Amendes aux plateformes; obligation de retrait.	• Deux types de protection : protection générale contre la reproduction numérique réaliste et droits précis pour les artistes-interprètes. • Réglemente le contenu d'images et d'audio, et est utilisé pour des questions liées aux hypertrucages à caractère sexuel. • Mise en œuvre par le biais de la législation sur les services numériques de l'UE. • Entrée en vigueur en juillet 2026.
Corée du Sud	*Loi relative aux cas spéciaux en matière de répression des infractions*	2024	Création et distribution d'IINC (y compris celles générées par l'IA)	Jusqu'à 7 ans d'emprisonnement.	• En réaction à la prolifération de contenus sexuels hypertruqués dans un groupe de clavardage dans Telegram comptant plus de 22 000 membres[38]. • Interdiction générale, y compris la consommation.
Royaume-Uni	*Loi sur les données (utilisation et accès)* (DUAA)[39]	2025	Création et sollicitation d'IINC (y compris celles facilitées par l'IA)	Jusqu'à 6 mois + amendes illimitées.	• S'appuie sur des lacunes antérieures (Loi de 2015 sur la « pornographie de vengeance », Loi de 2023 sur la sécurité en ligne). • Fruit d'un travail de défense des intérêts.

Malgré de récentes avancées législatives dans certains pays comme le Canada, l'architecture réglementaire plus large demeure souvent structurellement incomplète. Quels que soient les pays, six lacunes structurelles ressortent clairement des cadres normatifs relatifs à la violence fondée sur le sexe (VFS) facilitée par la technologie : 1) des définitions fragmentées et incohérentes, 2) la prédominance d'engagements non contraignants par rapport aux obligations exécutoires, 3) des progrès régionaux inégaux, 4) des retards entre l'adoption et la mise en œuvre, 5) une responsabilité limitée des plateformes et de l'IA, et 6) des lacunes persistantes en matière de données et de suivi[40].

Les tendances susmentionnées façonnent les lois de trois manières principales : 1) plusieurs pays continuent de s'appuyer sur des dispositions étroites, propres à certaines infractions, plutôt que sur des cadres juridiques intégrés, 2) les lois relatives à la cybercriminalité et à la sécurité en ligne n'intègrent souvent pas une perspective soucieuse des sexospécificités, et 3) les mécanismes d'application sont faibles en raison de capacités institutionnelles limitées et de l'absence d'obligations contraignantes pour les entreprises de technologies.

Tendances courantes dans la réglementation du matériel pédopornographique

Le paysage réglementaire pour les images d'abus pédosexuels a grandement évolué au cours des dernières années, mais des lacunes critiques demeurent, en particulier dans le cas du contenu généré numériquement. Un examen effectué en 2023[41] a permis d'évaluer les lois nationales de 196 pays en tenant compte de 5 critères : 1) la criminalisation des images d'abus pédosexuels, 2) la définition juridique, 3) la criminalisation des infractions facilitées par les technologies, 4) l'interdiction de la possession, indépendamment de l'intention de distribution et 5) l'obligation de signalement pour les fournisseurs d'accès à Internet. L'étude a montré que seuls 32 % des pays disposaient d'une loi et que, parmi ceux-ci, 40 % ne traitaient pas des infractions facilitées par les technologies. Seuls 27 pays sur 196 satisfaisaient aux cinq critères, dont le Canada. Le Mexique en satisfaisait quatre, mais ne respectait pas l'obligation de signalement pour les fournisseurs d'accès à Internet.

Les lacunes sont encore plus importantes dans le cas d'images d'abus pédosexuels générées numériquement. Une étude[42] menée en 2024 portant sur 49 pays a révélé que neuf d'entre eux ne criminalisaient pas explicitement ce type de matériel d'abus sexuel sur des enfants qui sont générées numériquement ou avec l'IA. Dans cinq de ces pays, leur traitement dépend du contexte, et dans quatre autres, dont le Mexique, leur légalité dépend de la présence ou non d'enfants réels dans les images, excluant ainsi du cadre juridique le contenu synthétique ne comportant aucune personne survivante identifiable.

Une enquête menée auprès de personnes ayant recherché des images d'abus pédosexuels sur le Web caché a révélé que près de trois personnes sur dix ont déclaré avoir visionné ces contenus préjudiciables aux personnes mineures facilitées par l'IA, tandis qu'une personne sur dix a admis en avoir créé elle-même avec un minimum d'effort[43].

États-Unis : la loi *TAKE IT DOWN* et au-delà

La réglementation des images intimes non consensuelles et des images d'abus pédosexuels aux États-Unis est particulièrement pertinente pour le Canada et le Mexique. Leurs écosystèmes numériques sont intimement interconnectés aux plateformes situées aux États-Unis et leurs approches réglementaires sont façonnées par leurs engagements en vertu du chapitre portant sur le commerce numérique[44] de l'Accord Canada–États-Unis–Mexique (ACEUM).

Avant 2025 aux États-Unis, en vertu de l'article 230 de la *Communications Decency Act* (Loi sur la décence dans les communications), les personnes survivantes faisaient face à un ensemble disparate de lois étatiques, à des recours fédéraux limités et à l'immunité des plateformes pour le contenu de tiers[45]. L'adoption de deux lois bipartites historiques en 2025-2026 est venue changer cette situation. Le tableau 2 présente les nouvelles lois américaines traitant des IINC facilitées par l'IA.

Lois américaines pour lutter contre les IINC facilitées par l'IA

Instrument	Date d'adoption	Droit	Dispositions principales
TAKE IT DOWN Act[46] (Outils pour lutter contre l'exploitation avérée en empêchant la distribution d'hypertrucages technologiques sur les sites Web et les réseaux)	2025	Criminel	• Criminalisation de la publication intentionnelle d'IINC (y compris celles facilitées par l'IA). • Obligation pour les plateformes de retirer les IINC dans un délai de 48 heures. • Sanctions pécuniaires et peine d'emprisonnement pouvant aller jusqu'à deux ans. • Sanctions plus lourdes pour les affaires impliquant des personnes mineures.
DEFIANCE Act[47] (Outil pour stopper les images explicites falsifiées et les modifications sans consentement)	2026	Civil	• Options élargies offertes aux personnes survivantes au-delà du cadre de la justice pénale. • Possibilité d'intention d'une poursuite civile pour obtenir réparation pour les préjudices financiers et émotionnels[48].

Il reste toutefois des défis à relever dans leur mise en œuvre. L'efficacité du retrait du contenu dépend d'une vérification rigoureuse de l'identité afin de prévenir la fraude, tandis que le délai de 48 heures, jugé insuffisant, met à l'épreuve les plateformes sans leur offrir de garanties en matière de financement ou de conformité. De plus, la portée extraterritoriale de ces deux lois dépend de la coopération des acteurs mondiaux, et ce, dans un contexte de fragmentation et de tensions géopolitiques grandissantes[49].

En ce qui concerne la protection des personnes mineures, le Sénat américain a adopté à l'unanimité le *STOP CSAM Act of 2025*[50] (la Loi de 2025 pour stopper les images d'abus pédosexuels) qui élargit la responsabilité des plateformes en introduisant un critère d'imprudence, ce qui signifie que les plateformes peuvent être tenues responsables de l'hébergement ou de la facilitation de la distribution d'images d'abus pédosexuels, et ce, même en l'absence de connaissance explicite. La loi vise la promotion active et le stockage passif de ce type de matériel, y compris le matériel facilité par l'IA, comblant ainsi une lacune qui permettait auparavant aux plateformes d'échapper à leur responsabilité en invoquant leur ignorance. Les personnes qui s'y opposent mettent toutefois en garde contre le fait que ces nouvelles dispositions pourraient être utilisées par les entreprises pour justifier un affaiblissement ou l'abandon du chiffrement de bout en bout, ce qui entraînerait des répercussions plus larges sur la protection de la vie privée des utilisatrices et utilisateurs, et la sécurité des communications[51].

Parallèlement à ces avancées sur le plan législatif, le National Center for Missing & Exploited Children (NCMEC) a introduit deux outils complémentaires : le service *Take it Down*[52], qui permet aux personnes mineures de demander le retrait de contenu intime sans implication policière ni action judiciaire formelle, et CyberTipline[53], un système de signalement national centralisé des cas d'exploitation sexuelle d'enfants en ligne ciblant le pédopiégage, la traite des personnes, les images d'abus pédosexuels et le contenu facilité par l'IA. Toutefois, certaines limites existent, notamment le fait qu'il ne vise que les formats image et vidéo, excluant ainsi les fichiers audio ou texte[54].

PROFIL DU PAYS: CANADA

Cette section s'intéresse au paysage des IINC, incluant les images d'abus pédosexuels, au Canada. Elle décrit les mécanismes légaux, réglementaires et de dépôt de plaintes actuellement en place, et cerne les principales lacunes pour contrer la création et la distribution d'IINC facilitées par l'IA.

Aperçu de l'exploitation des images intimes non consensuelles au Canada

En 2022, les services de police ont enregistré 896 cas rapportés de distribution d'IINC[55]. Or, des estimations plus générales suggèrent qu'il y aurait environ 275 000 personnes survivantes et 2,37 millions d'images de type IINC par an[56].

Malgré ces chiffres, d'importantes lacunes demeurent dans les données. Les données désagrégées (données selon des variables démographiques précises, telles que le genre, le sexe, le lieu de résidence, l'appartenance ethnique, etc.) sur les IINC facilitées par l'IA ne sont pas disponibles, ce qui rend difficile d'évaluer l'évolution de ce phénomène parallèlement à l'adoption rapide de l'IA générative. Même si le Canada n'a pas connu un cas marquant ayant fait les manchettes, le problème est bien documenté et prend de l'ampleur, avec des répercussions évidentes sur la dignité, la vie privée, la santé et la participation des jeunes femmes à la vie publique.

L'encadré suivant décrit certains cas publics d'IINC facilitées par l'IA survenus au pays.

Cas d'IINC facilitées par l'IA au Canada

→ **Un Québécois condamné pour pornographie juvénile facilitée par l'IA (2023)**[57]

Un homme a été condamné à huit ans de prison pour avoir utilisé l'IA pour créer des vidéos d'images d'abus pédosexuels. Il a plaidé coupable à la production d'au moins sept vidéos hypertruquées et à la possession de plus de 545 000 fichiers d'images d'abus pédosexuels. Alors que la défense a plaidé en faveur d'une peine moins sévère étant donné qu'aucune violence corporelle n'avait été commise, le juge a estimé que la création de ce type de matériel constituait une nouvelle atteinte à l'intégrité sexuelle des personnes survivantes.

→ **Photos facilitées par l'IA de jeunes filles nues d'une école de Winnipeg publiées en ligne (2023)**[58]

En 2023, on a découvert que des IINC facilitées par l'IA d'étudiantes mineures d'une école de Winnipeg circulaient sur Internet. L'école a alerté les familles, contacté le service de police et activé les protocoles de soutien aux personnes survivantes, tout en faisant appel à Cybertip.ca et au Projet Arachnid pour signaler et faire retirer le contenu[59]. Aucune accusation n'a été portée, le service de police invoquant des défis liés à l'obtention d'éléments de preuve, la réticence des personnes survivantes à entamer des poursuites, la faible probabilité de condamnation et les complexités juridiques liées au contenu facilité par l'IA[60].

→ **Des étudiants de l'école London Catholic publient des faux nus (2024)**[61]

Des étudiants d'une école secondaire locale ont partagé dans des groupes de clavardage des IINC facilitées par l'IA de leurs collègues féminines. Le service de police a ouvert une enquête et l'école a menacé de prendre des mesures disciplinaires. Or, plusieurs mois plus tard, aucune accusation au criminel n'avait été portée contre les étudiants impliqués. Le Conseil scolaire catholique du district de London n'a pas précisé si des mesures disciplinaires avaient été prises et a refusé de répondre aux questions des journalistes[62].

Cadre réglementaire

La *Loi visant à protéger les victimes* (projet de loi C-16) est entrée en vigueur le 18 juin 2026. Cette Loi modifie le *Code criminel* et d'autres textes législatifs afin de répondre aux menaces modernes et de renforcer la protection des victimes. Selon le ministère de la Justice du Canada, il s'agit de « *l'une des réformes du Code criminel les plus importantes depuis des générations pour remédier aux délais judiciaires, protéger les victimes et personnes survivantes de violence fondée sur le sexe, y compris la violence sexuelle et la violence entre partenaires intimes, et pour garder les enfants à l'abris des personnes prédatrices*[63] ».

La Loi touche à plusieurs lois pénales et correctionnelles, dont certaines dispositions relatives à la diffusion d'IINC facilitées par l'IA. Plus précisément, elle élargit l'infraction de distribution d'IINC pour inclure les représentations visuelles créées par des moyens mécaniques ou électroniques (deepfakes). La définition « d'images intimes » du *Code criminel* couvre désormais le contenu synthétique facilité par l'IA, ce qui en rend l'infraction plus facile à faire respecter. La Loi rétablit aussi des peines minimales obligatoires pour plusieurs infractions, dont la diffusion d'IINC et le voyeurisme. Elle crée aussi de nouvelles infractions, notamment la menace de diffusion de matériel d'abus et d'exploitation pédosexuels, y compris les hypertrucages, et la menace de diffusion d'IINC, y compris également les hypertrucages à caractère sexuel[64].

Dans les mois à venir, il sera crucial d'évaluer l'efficacité de ces nouvelles mesures ainsi que les ressources allouées à leur mise en œuvre, notamment pour la formation des juristes, des corps policiers et du personnel qui intervient auprès des personnes victimes.

Cette nouvelle loi vise les personnes contrevenantes, sur une base individuelle, contrairement au projet de loi C-63 (*la Loi édictant la Loi sur les préjudices en ligne*), qui visait plutôt à imposer des obligations réglementaires aux plateformes. Le projet de loi C-63 est mort au Feuilleton en 2025 lors de la dissolution du Parlement, menant aux dernières élections fédérales. Le projet de loi C-34 (*Loi sur les médias sociaux sécuritaires*), déposé en juin 2026, reprend cette approche réglementaire afin de lutter plus efficacement contre les préjudices numériques[65].

En attente de nouvelles obligations réglementaires des plateformes

Le 10 juin 2026, le gouvernement du Canada a déposé un nouveau projet de loi, C-34 (*Loi sur les médias sociaux sécuritaires*), visant donner de nouvelles obligations aux plateformes afin de mieux répondre aux contenus préjudiciables en ligne, incluant les hypertrucages.

La Loi sur les médias sociaux sécuritaires promulguerait deux nouvelles lois : la *Loi sur la sécurité numérique* et la *Loi sur la Commission canadienne de la sécurité numérique*. Sa portée dépasse celle de C-63 : en plus des services de médias sociaux, elle couvrirait les services d'agents conversationnels dotés d'intelligence artificielle, ainsi que d'autres services en ligne, sites Web et applications non couverts par les deux premières catégories. Toutefois, en date du présent rapport, le projet de loi est à un stade préliminaire de son parcours parlementaire (étape de la première lecture). Ses dispositions pourraient encore faire l'objet de modifications importantes. Plusieurs zones grises restent à clarifier[66].

Protection de la vie privée

Le Commissariat à la protection de la vie privée du Canada propose une approche fondée sur la protection des données plutôt que sur le droit pénal. Lorsque des données personnelles ou une image d'une personne sont utilisées sans consentement pour générer du contenu synthétique à caractère sexuel, le commissaire peut enquêter sur la conformité des organisations, imposant des obligations aux entités impliquées dans la création et la distribution de ce contenu, et non pas uniquement aux personnes à l'origine du contenu[67]. Cette approche a pris tout son sens après que le commissaire a ouvert une enquête sur xAI et X concernant l'utilisation de leur outil Grok pour générer des IINC au début de l'année 2026[68].

Les cadres provinciaux

Les cadres provinciaux, quant à eux, varient considérablement dans leur capacité à lutter contre les IINC facilitées par l'IA. Par exemple, la *Loi visant à contrer le partage sans consentement d'images intimes*[69] du Québec, en vigueur depuis juin 2025, définit explicitement une image intime comme « toute image, modifiée ou non, représentant ou semblant représenter une personne soit nue […], soit se livrant à une activité sexuelle explicite ». Cette formulation étend la portée de la Loi aux contenus modifiés numériquement et potentiellement synthétiques, à l'instar de ce qui a été adopté par d'autres provinces dans des cadres semblables, notamment l'*Intimate Images Protection Act*[70] (Loi sur la protection des images intimes) de la Colombie-Britannique), qui permet aux personnes survivantes de demander à la fois le retrait du contenu et des réparations civiles, et de bénéficier d'un service d'accompagnement institutionnel, la *Loi sur la communication illégale d'images intimes* SNB 2022[71] du Nouveau-Brunswick et l'*Intimate Images Protection Act* RSPEI 1988 (Loi sur la protection des images intimes) de l'Île-du-Prince-Édouard[72]. En revanche, le langage employé dans les cadres réglementaires de l'Alberta et de la Nouvelle-Écosse est trop restrictif pour couvrir explicitement le contenu modifié ou généré par l'IA, bien que cette dernière province gère Cyberscan[73], un centre de ressources voué à la lutte contre l'exploitation d'images intimes. L'Ontario ne dispose d'aucun cadre provincial en la matière.

En ce qui concerne les personnes mineures, l'Ontario et le Québec exigent des établissements d'enseignement postsecondaire qu'ils se dotent de politiques de lutte contre les violences sexuelles, tandis que la plupart des autres provinces laissent cette question à la discrétion des établissements. Même si ces politiques offrent des possibilités de retrait de contenu et des réparations, elles n'abordent généralement pas les séquelles psychologiques à long terme subies par les personnes survivantes ni les dimensions structurelles plus larges[74].

La structure fédérale du Canada ajoute une couche supplémentaire de complexité. Le droit pénal relève de la compétence fédérale, mais l'application de la loi est principalement du ressort des provinces, sans clause de suprématie[75]. Les cadres réglementaires civils provinciaux, qui ont des niveaux de protection différents d'une province à l'autre, coexistent bien avec le droit criminel fédéral, mais ce système peut être complexe. Il en résulte un système dans lequel les cadres réglementaires civils les plus protecteurs sont concentrés dans une poignée de provinces et où l'accès à la justice pour les personnes survivantes dépend fortement de leur lieu de résidence.

Mécanismes de dépôt de plaintes et de réparation

Le paysage canadien en matière de réparation offre aux personnes survivantes des voies d'accès utiles, mais inégalement réparties sur le territoire. Les mécanismes les plus solides sont offerts à l'échelle provinciale, la surveillance du gouvernement fédéral jouant un rôle complémentaire, mais limité.

L'*ordonnance de cessation ou de prévention*[76] du Québec se distingue comme étant le mécanisme d'intervention d'urgence le plus structuré au pays. Ce mécanisme permet de déposer des demandes accélérées et sommaires pour faire cesser ou prévenir le partage en remplissant des formulaires officiels en ligne, ce qui réduit les obstacles procéduraux pour les personnes survivantes ne bénéficiant pas d'une représentation juridique et autorise des mesures exceptionnelles lorsque l'urgence exige une intervention immédiate. L'*Intimate Images Protection Act* (Loi sur la protection des images intimes) de la Colombie-Britannique offre aussi un soutien institutionnel qui accompagne les personnes survivantes tout au long du processus ainsi qu'un soutien émotionnel et un aiguillage vers des services de soutien[77].

Pour les affaires impliquant des personnes mineures, Cybertip.ca[78], la centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet, gérée par le Centre canadien de protection de l'enfance, offre un canal de signalement des infractions comme les images d'abus pédosexuels, le leurre en ligne, la sextorsion et, explicitement, les IINC facilitées par l'IA. La plateforme gère aussi Projet Arachnid, un outil technologique qui envoie chaque mois des milliers d'avis de retrait de contenu aux plateformes hébergeant des images d'abus pédosexuels.

Avancées et lacunes en matière de réglementation, de mise en œuvre et de coordination

La réponse du Canada aux IINC facilitées par l'IA demeure limitée par un ensemble de contraintes structurelles qui compromettent son efficacité dans la pratique :

→ **Cadres réglementaires en matière de protection de la vie privée dépassés**

Le régime réglementaire canadien, largement conçu dans un contexte pré-IA générative, est de moins en moins adapté pour relever les défis posés par le contenu synthétique. Cette limitation est particulièrement critique pour les enfants et les adolescentes et adolescents pour qui l'exposition à des images d'abus pédosexuels facilitées par l'IA dépasse les situations pour lesquelles les cadres existants ont été conçus[79].

De plus, les lois existantes en matière de protection de la vie privée ne prévoient pas de mécanismes d'application efficaces, notamment des sanctions pénales et des sanctions pécuniaires administratives. Par conséquent, le cadre actuel s'apparente davantage à un ensemble de normes volontaires qu'à un régime réglementaire contraignant, et ce, malgré l'existence de propositions de réforme.

→ **Fragmentation institutionnelle et contraintes en matière de capacités**

La réponse du Canada est affaiblie par la fragmentation des cadres juridiques et institutionnels. L'application des dispositions pénales, les recours au civil et les mesures de protection de la vie privée s'inscrivent dans des régimes largement disjoints (*Code criminel*, systèmes civils provinciaux et surveillance de la protection des données), sans mécanisme global garantissant leur cohérence. Par conséquent, l'accès des personnes survivantes à des mesures de réparation et de protection varie considérablement selon la province et la voie juridique[80].

Les capacités des institutions constituent une autre contrainte. Au Canada, la décision d'engager des poursuites pénales revient aux procureures et procureurs de la Couronne plutôt qu'au service de police, ce qui crée un filtre institutionnel additionnel et entraîne un décalage entre l'enquête et la mise en accusation. En outre, les cas reposent souvent sur la nécessité d'expliquer des technologies complexes à des tribunaux disposant d'une expertise technique limitée, alors que les membres des services de police ne reçoivent qu'une formation limitée dans des domaines comme l'informatique judiciaire et les abus qui sont perpétrés spécifiquement sur des plateformes. Ces défis sont aggravés par le manque de ressources, des protocoles de documentation peu clairs et l'incertitude entourant les seuils juridiques applicables aux preuves numériques[81].

→ **Identification des personnes à l'origine des IINC et cas inter-juridictionnelles**

L'identification des personnes à l'origine de la distribution d'IINC reste l'un des principaux obstacles opérationnels. Si les cas impliquant des formes courantes d'IINC peuvent être traçables, l'attribution de la responsabilité s'avère souvent difficile, voire impossible, dans les cas facilités par l'IA. Ce défi est particulièrement important dans les cas inter-juridictionnels, où les autorités nationales ont une portée limitée.

→ **Lacunes en prévention et en réponses institutionnelles**

Les mesures préventives et éducatives restent également inégales. Bien que certains programmes scolaires provinciaux abordent les questions de violences sexuelles et de préjudices numériques, leur mise en œuvre n'est pas uniforme et dépend souvent des enseignantes et enseignants eux-mêmes ainsi que des politiques locales. Au niveau postsecondaire, les cadres spécifiques de prévention des violences sexuelles ont été affaiblis depuis 2021, souvent intégrés dans des initiatives plus larges portant sur l'équité, la diversité et l'inclusion (EDI).

→ **Inégalités en matière d'accès à la justice**

L'accès à la justice constitue un autre obstacle. Les personnes disposant de ressources financières plus importantes, d'un capital social plus développé ou d'une meilleure connaissance des systèmes juridiques sont mieux placées pour demander réparation et s'y retrouver dans les mécanismes proposés. En revanche, les communautés des Premières Nations et les communautés racialisées font face à des obstacles systémiques supplémentaires, notamment une méfiance historique à l'égard des forces de l'ordre et du système judiciaire, ce qui réduit considérablement les taux de signalement et l'accès à du soutien.

PROFIL DU PAYS : MEXIQUE

Cette section s'intéresse aux enjeux et encadrements des IINC, incluant les images d'abus pédosexuels, au Mexique. Elle décrit les mécanismes réglementaires et de dépôt de plaintes actuellement en place, et cerne les principales lacunes pour contrer la création et la distribution des IINC facilitées parl'IA.

Aperçu de l'exploitation des images intimes non consensuelles au Mexique

Les dernières estimations indiquent que 84,46 % des personnes survivantes sont des femmes, celles âgées de 21 à 35 ans représentant près du tiers des cas[82]. De plus, 43,2 % des femmes et des filles qui sont victimes de cyberharcèlement signalent avoir été menacées avec la publication de données personnelles ou d'image intimes comme forme d'extorsion, des hommes cisgenres étant impliqués dans 80 % des incidents et identifiés comme principaux agresseurs dans 70 % [83].

L'exposition aux abus en ligne commence également très tôt. Les jeunes femmes âgées de 18 à 24 ans sont 27 % plus susceptibles d'être victimes de violence en ligne que leurs homologues masculins[84]. La plupart des filles déclarent avoir vécu leur première expérience de harcèlement en ligne entre 14 et 16 ans, près de la moitié d'entre elles ayant reçu des menaces de violence physique ou sexuelle[85].

Comme le Mexique se classe parmi les cinq premiers pays au monde pour ce qui est du trafic vers les sites Web les plus visités hébergeant des IINC, l'ampleur des préjudices est accentuée par une forte consommation[86]. Le Mexique figure aussi parmi les pays affichant les taux mondiaux les plus élevés de production et de distribution d'images d'abus pédosexuels, l'impact est donc particulièrement important pour les personnes mineures. La ville de Ciudad Juárez, dans le nord du pays, est à elle seule le lieu d'origine de 60 % des fichiers d'images d'abus pédosexuels identifiés à l'échelle mondiale[87].

De plus, les cas signalés ont augmenté de 86 % au cours de la première moitié de 2025, les filles représentant 59 % des personnes concernées[88].

L'encadré suivant décrit les deux cas les plus connus d'IINC facilitées par l'IA survenus au pays.

Cas d'IINC facilitées par l'IA au Mexique

→ **Le cas de l'IPN (2023)**[89]
Une affaire d'IINC facilitées par l'IA de grande envergure a été mise au jour à l'Instituto Politécnico Nacional (IPN), où les autorités ont découvert 166 000 fichiers synthétiques, y compris 20 000 vidéos, dont au moins 40 % mettaient en scène des étudiantes âgées de 17 à 25 ans. Un étudiant a d'abord été arrêté pour violence sexuelle numérique, mais une partie de la condamnation a ensuite été renversée faute de preuves suffisantes. Après que les autorités ont confirmé que du matériel impliquait des personnes mineures, les accusations de possession et de distribution d'images d'abus pédosexuels ont conduit à une peine de cinq ans de prison et à une amende. Cette affaire reste partiellement non résolue, un processus d'appel étant en cours et les personnes survivantes dénonçant une négligence institutionnelle et une revictimisation.

→ **L'affaire Zacatecas (2025)**[90]
Au moins 400 étudiantes d'une école secondaire technique de l'État mexicain de Zacatecas ont signalé la création et la distribution d'IINC facilitées par l'IA. Les enquêtes semblent indiquer que trois adolescents fréquentant aussi cet établissement ont créé et diffusé ce contenu, mais au moment de la préparation de ce rapport, aucune condamnation n'avait encore été prononcée.

Cadre réglementaire

Le Mexique dispose de l'un des cadres juridiques les plus complets au monde en matière de lutte contre la violence numérique. L'un de ses piliers centraux est la *Ley Olimpia*[91] (Loi Olimpia), un ensemble de réformes législatives entamées en 2018 qui ont permis d'établir la violence numérique en tant que catégorie reconnue sur le plan juridique et de criminaliser les atteintes à l'intimité sexuelle par des moyens numériques, y compris la distribution d'IINC. Bien que ces réformes aillent au-delà des images authentiques pour inclure le contenu modifié, permettant ainsi d'intégrer les IINC facilitées par l'IA dans des définitions existantes, leur application au contenu synthétique demeure en pratique inégale.

D'abord adoptée dans l'État de Puebla en 2018, la *Ley Olimpia* a depuis été mise en œuvre dans l'ensemble des 32 États mexicains grâce à des modifications apportées aux codes pénaux étatiques, criminalisant les IINC à l'échelle nationale. Appuyé sur des définitions juridiques et une terminologie variables, cet élargissement entraîne cependant des incohérences dans la manière dont ces infractions sont définies, font l'objet d'enquêtes et sont poursuivies[92].

Des modifications apportées à la *Ley General de Acceso de las Mujeres a una Vida Libre de Violencia*[93] (Loi générale sur l'accès des femmes à une vie exempte de violence) et au *Código Penal Federal*[94] (Code pénal fédéral) en 2021 ont renforcé le cadre fédéral. Ces réformes ont officiellement intégré la violence numérique dans le cadre juridique national et élargi les outils de prévention et de réparation, mais elles ne couvrent pas explicitement les IINC facilitées par l'IA.

Dans les cas impliquant aussi de l'exploitation, la *Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos*[95] (Loi générale visant à prévenir, sanctionner et éradiquer les délits liés à la traite des personnes et à assurer la protection et l'assistance aux victimes de ces délits) prévoit des restrictions concernant la pornographie non consensuelle, en particulier lorsqu'elle implique une exploitation sexuelle, des personnes mineures ou des personnes en situation de handicap, ou lorsque des tiers tirent profit du contenu. Ces dispositions peuvent s'appliquer dans certains cas d'IINC, souvent prévoyant des peines plus lourdes et s'appuyant sur des mécanismes institutionnels plus solides que les dispositions standards relatives à la violence numérique[96].

Enfin, malgré de récentes avancées réglementaires, la protection des enfants contre la violence numérique reste limitée. Le Code pénal fédéral[97] définit la pédopornographie comme tout acte impliquant le trafic, la distribution ou l'exposition de personnes mineures par le biais de photographies, d'images, d'écrits ou d'enregistrements, qu'ils soient réels ou simulés, commis par une personne utilisant tout moyen ou toute méthode. De même, toute personne qui stocke, achète ou loue ce type de contenu sans intention de le vendre ou de le distribuer est passible d'une peine d'emprisonnement d'un à cinq ans, en plus d'amendes[98].

Mécanismes de dépôt de plaintes et de réparation

Sur le plan judiciaire, la Cour suprême du Mexique a établi un protocole pour traiter les cas dans une perspective soucieuse des sexospécificités[99]. Ce protocole guide les tribunaux dans l'examen du contexte, l'évaluation des faits et des éléments de preuve, l'identification des formes de discrimination intersectionnelle, la reconnaissance des stéréotypes et des préjugés liés au genre, ainsi que la détermination des réparations[100]. Dans les affaires civiles, l'article 1916 du Code civil fédéral[101] prévoit la possibilité d'obtenir des dommages-intérêts moraux, une voie de recours accessible aux personnes survivantes de la distribution d'IINC qui souhaitent une alternative aux poursuites pénales.

Sur le plan institutionnel, la ville de Mexico est le seul territoire à disposer d'un organisme spécialisé dans les crimes sexuels numériques[102], mais il fait face à plusieurs défis. Non seulement il dépend d'un soutien externe pour les enquêtes techniques, mais son personnel est principalement formé en matière de traite des personnes, ce qui reflète un manque d'expertise numérique spécialisée. Le service téléphonique *Línea Mujeres*[103] offre des conseils et un soutien aux femmes victimes de violence, mais lorsque les cas impliquent des violences numériques, elles sont dirigées vers la cyberpolice de la Garde nationale, qui n'est pas spécialisée dans les questions de genre.

La protection des personnes mineures, quant à elle, est coordonnée par le System national de

protection des enfants et des adolescents[104], mais ce système n'a pas été conçu pour traiter spécifiquement les cas d'IINC facilitées par l'IA.

La société civile comble bon nombre des lacunes laissées par les mécanismes institutionnels. Des organisations comme *Cultivando Género*[105], *Defensoras Digitales*[106], *Hijas de Internet*[107], *Luchadoras*[108] et *SocialTic*[109], entre autres, proposent des formations à la sécurité numérique, des ressources de prévention et un soutien direct aux personnes survivantes là où les institutions officielles sont absentes, insuffisantes ou inaccessibles.

Mise à jour réglementaire d'octobre 2026 : nouvelles obligations pour les plateformes numériques

Le Mexique a adopté un décret imposant de nouvelles obligations aux plateformes numériques pour protéger les personnes mineures contre les contenus préjudiciables, notamment des mesures de vérification de l'âge et de retrait de contenus.

Bien qu'obligatoire, le décret ne définit pas de critères techniques suffisamment détaillés pour sa mise en œuvre et sa supervision, ni ne prévoit de sanctions spécifiques en cas de non-respect. Le gouvernement l'a présenté comme non punitif et a indiqué qu'il pourrait proposer une loi prévoyant des sanctions si les plateformes ne respectent pas leurs obligations.

Bien que le décret ne traite pas explicitement des IINC, certaines de ses dispositions pourraient s'appliquer lorsque des personnes mineures sont concernées. Ce décret illustre les difficultés persistantes à traduire les obligations réglementaires en mécanismes efficaces de responsabilisation des plateformes.

Source : *Presidencia de la República (14 octobre 2026), Presidenta Claudia Sheinbaum firma decreto de entornos digitales seguros para niñas, niños y adolescentes.*

Lacunes en matière de réglementation, de mise en œuvre et de coordination

Malgré les mécanismes décrits ci-dessus, la réponse du Mexique aux IINC facilitées par l'IA se heurte à une série de limitations structurelles qui révèlent un décalage profond entre l'étendue du cadre juridique et la capacité institutionnelle à le mettre en œuvre.

→ **Mise en œuvre avant législation**

Au Mexique, le problème fondamental n'est pas un manque de normes, mais bien la capacité institutionnelle limitée à les mettre en œuvre. Les procureures et procureurs manquent souvent de clarté quant aux preuves à demander et à la manière d'intégrer ces infractions dans une enquête ou de monter des dossiers capables de résister à l'examen judiciaire. Plusieurs bureaux de procureures et procureurs évitent tout simplement les cas d'IINC, craignant que les juges n'exigent des normes de preuve équivalentes à celles requises dans les affaires de traite des personnes, normes qui sont non seulement disproportionnées par rapport aux peines encourues, mais aussi souvent inadaptées aux IINC facilitées par l'IA, où les formes traditionnelles de preuve peuvent ne pas exister.

Une autre complication réside dans la terminologie elle-même. L'infraction est définie sous différentes appellations, ce qui permet aux procureures et procureurs d'interpréter et de classer les comportements selon leurs propres critères. Cette variabilité dans l'interprétation introduit une incohérence dès le tout premier contact avec les institutions et peut déterminer si un cas sera ou non poursuivi. Sur les 1500 plaintes déposées en 2021 pour distribution d'IINC, seules 8 ont été renvoyées devant un juge afin d'engager officiellement une poursuite au criminel devant les tribunaux, ce qui représente 0,5 % des cas[110]. Plusieurs affaires ont plutôt donné lieu à des accords conditionnels ou à des jugements sommaires, mais leur nombre reste inconnu.

→ **Lacunes judiciaires et en matière de capacités institutionnelles**

Les autorités publiques manquent souvent de formation technique et sur les sexospécificités, ce qui limite leur capacité à lutter efficacement contre les abus en ligne. Cette situation se traduit par une pénurie de personnel spécialisé ainsi que par l'absence de protocoles clairs et normalisés[111]. Dans la pratique, ces lacunes peuvent décourager les signalements, en particulier lorsque les personnes survivantes anticipent une revictimisation, une crainte encore aggravée par la tendance persistante à minimiser les préjudices numériques en les qualifiant de « non réels » lorsque le contenu est synthétique.

→ **Fardeau de la preuve sur les personnes survivantes**

Les personnes survivantes sont souvent tenues de prouver leur crédibilité, de recueillir et de conserver elles-mêmes leurs éléments de preuve, et de s'y retrouver dans des procédures complexes en matière de preuves numériques, gérant les captures d'écran, les métadonnées, la conservation des adresses URL, les procédures des plateformes et les incohérences pangouvernementales[112]. Contrairement aux cas impliquant des préjudices physiques, les dommages psychologiques, financiers, sociaux et professionnels causés par les IINC sont difficiles à quantifier à l'aide des outils de preuve standards.

→ **Lacunes en matière de protection des personnes mineures**

La Ley General de Educación[113] (Loi générale sur l'éducation) du Mexique exigent des établissements scolaires qu'ils se dotent de protocoles de prévention et d'intervention en matière de violence, mais ceux-ci n'ont pas été adaptés pour traiter les abus par le biais d'images, la violence numérique ou le contenu facilité par l'IA. Les établissements scolaires ont mis en place des campagnes de lutte contre l'intimidation traditionnelle, mais ne les ont pas non plus transposées dans l'espace numérique.

→ **Lacunes en matière de données et de preuves**

Au Mexique, le paysage des données est insuffisant pour permettre l'élaboration de politiques fondées sur des données probantes. Les données relatives à la cybersécurité fournies par l'Institut national de statistique et de géographie (INEGI) ne présentent pas le niveau de détail nécessaire pour lutter contre les IINC facilitées par l'IA. Il n'existe pas d'indicateurs fiables permettant de distinguer les contenus synthétiques des contenus réels, pas de suivi de bout en bout des cas, de leur signalement à leur résolution, ni de données publiques exhaustives sur le profil des personnes à l'origine des infractions (p. ex., âge, sexe et lien avec les personnes survivantes).

PRINCIPAUX CONSTATS COMPARATIFS

Les mesures prises par le Canada et le Mexique pour lutter contre les IINC facilitées par l'IA révèlent un paradoxe commun aux deux pays. Bien qu'ils s'appuient sur des traditions juridiques, des architectures institutionnelles et des contextes en matière de ressources très différents, les résultats pour les personnes survivantes sont, au bout du compte, semblables dans les deux pays, comme le montre le tableau ci-dessous.

Constats comparatifs des réponses du Canada et du Mexique dans la lutte contre les IINC facilitées par l'IA

	Mexico	**Canada**	**Points communs**
Couverture juridique du contenu synthétique	En principe, *Ley Olimpia* vise le contenu modifié ou altéré; son application n'est toutefois pas uniforme dans les 32 États.	La *Loi visant à protéger les victimes* (projet de loi C-16, adopté) élargit la définition d'IINC prévue au *Code criminel* afin d'y inclure le contenu synthétique facilité par l'IA, y compris les hypertrucages à caractère sexuel. Elle criminalise également les menaces de distribuer des images intimes, y compris des hypertrucages à caractère sexuel.	• Les deux pays ont progressé vers la reconnaissance des préjudices facilités par l'IA dans le cadre de leurs régimes existants relatifs aux IINC. Toutefois, la réglementation demeure principalement axée sur les infractions individuelles et les conséquences préjudiciables, plutôt que sur l'ensemble de l'écosystème de génération et de diffusion par l'IA.
Responsabilité des plateformes et prévention	Obligations limitées spécifiques aux plateformes et une approche qui repose principalement sur des mécanismes de réparation par voie pénale et civile.	La responsabilité individuelle a été renforcée grâce à la *Loi visant à protéger les victimes* (projet de loi C-16, adopté), tandis que les obligations plus larges imposées aux plateformes continuent d'évoluer par l'entremise du projet de loi C-34 (*Loi sur les médias sociaux sécuritaires*), actuellement à l'étude dans le cadre du processus législatif.	• Aucun des deux pays ne dispose actuellement d'un cadre pleinement développé pour encadrer le rôle des plateformes dans la prévention, la détection et la réponse aux IINC générées par l'IA à grande échelle.
Capacités institution-nelles	Pratiquement inexistantes à l'extérieur de l'agence de la ville de Mexico chargée des crimes sexuels en ligne; aucune infrastructure spécialisée dans la majeure partie du pays.	Fragmentation entre les compétences fédérales et provinciales; disparités dans les capacités des procureures et procureurs de la Couronne et dans les compétences technologiques judiciaires.	• Les deux pays disposent d'un système judiciaire mal équipé pour gérer la complexité technique des cas d'IINC facilitées par l'IA.

	Mexico	Canada	Points communs
Mécanisme de réparation	L'article 1916 du *Code civil fédéral* comme moyen alternatif de réclamer des dommages-intérêts moraux. La société civile comble les lacunes majeures laissées par les institutions officielles.	Les mécanismes de signalement et de recours se concentrent principalement au niveau provincial. Le Québec et la Colombie-Britannique disposent de voies spécifiques permettant de demander le retrait ou la cessation de la diffusion d'images intimes. Pour les mineurs, Cybertip.ca offre un canal national spécialisé de signalement et de retrait de contenu.	• Les mesures de réparation centrées sur les personnes survivantes dépendent de leur lieu de résidence et des ressources disponibles, et non d'un cadre national cohérent.
Protection des personnes mineures	Un cadre juridique plus solide en vertu de la loi sur la traite des personnes; les personnes mineures qui commettent des infractions sont rarement poursuivies; les établissements scolaires ne sont pas préparés.	Les dispositions relatives aux images d'abus pédosexuels visent le contenu facilité par l'IA; le système de justice pénale pour les personnes mineures est souple; les mesures en milieu scolaire manquent de cohérence.	• Les deux pays disposent de cadres juridiques plus solides en matière d'images d'abus pédosexuels qu'en matière d'IINC chez les adultes, mais les établissements scolaires des deux pays n'ont pas su adapter leurs protocoles de prévention de la violence aux environnements numériques.
Données et preuves	Données désagrégées insuffisantes sur le contenu synthétique.	Des données agrégées sur les IINC existent; des indicateurs spécifiques à l'IA ne sont généralement pas disponibles; il n'existe pas de catégories de signalement normalisées.	• Aucun des deux pays ne peut mesurer pleinement l'ampleur des IINC facilitées par l'IA; les décideuses et décideurs élaborent donc des mesures pour réagir à un problème sans disposer de données suffisantes.
Accès à la justice pour les personnes survivantes	Le fardeau incombe aux personnes survivantes; la revictimisation est courante; seulement 0,5 % des plaintes aboutissent devant les tribunaux.	L'aide juridique coûte cher; le fardeau de la preuve incombe aux personnes survivantes; la honte dissuade les signalements; les groupes vulnérables font face à plusieurs obstacles.	• Dans les deux pays, un fardeau disproportionné incombe aux personnes survivantes; les personnes les plus marginalisées (les Premières Nations canadiennes, les populations autochtones mexicaines, les communautés racialisées, les personnes mineures) se heurtent aux plus grands obstacles pour accéder à la justice.

Le manque de responsabilité de la part des plateformes: un problème dans les deux pays

Parmi les points communs soulevés dans cette analyse comparative, aucun n'est plus important que la capacité limitée des deux pays à tenir les plateformes numériques responsables. Étant donné que la plupart des plateformes sur lesquelles sont créées, distribuées et monétisées les IINC facilitées par l'IA sont basées aux États-Unis, le Canada et le Mexique font face à une contrainte structurelle semblable en ce qui a trait à leur réglementation.

Ces défis sont accentués par le chapitre portant sur le commerce numérique de l'ACEUM, qui limite la capacité des gouvernements à imposer des exigences (comme la transparence algorithmique, la localisation des données ou la présence locale) aux plateformes, affaiblissant ainsi la souveraineté numérique et l'accès à la justice. Dans la pratique, les plateformes refusent souvent de fournir les informations nécessaires à l'identification des personnes à l'origine des IINC, invoquant leurs obligations en matière de protection de la vie privée. Même lorsque le contenu est retiré, il réapparaît fréquemment et les plateformes ne subissent guère de conséquences et ne bénéficient pas d'incitatifs pour améliorer la détection et l'application de la loi.

La nature transfrontalière des préjudices vient exacerber ces défis. Lorsque les personnes à l'origine des IINC agissent au-delà des frontières, les recours juridiques deviennent beaucoup plus complexes. Bien qu'il soit possible de déposer des plaintes, l'extradition est rarement envisageable, puisque les infractions liées aux IINC sont souvent classées comme des infractions mineures dans les cadres de coopération internationale. Par conséquent, plusieurs cas restent dans les faits hors de portée des autorités chargées de l'application de la loi, quelle que soit la rigueur de la législation nationale.

RECOMMANDATIONS EN MATIÈRE DE POLITIQUES PUBLIQUES

Le Canada et le Mexique sont aux prises avec des contraintes structurelles qu'aucun cadre national ne peut résoudre à lui seul : des plateformes basées aux États-Unis exerçant leurs activités au-delà de leur champ de compétence réglementaire, des incohérences dans les définitions qui compliquent la coopération transfrontalière et des lacunes en matière de protection des personnes mineures qui nécessitent des mesures éducatives coordonnées. Les recommandations suivantes visent à relever ces défis communs par le biais de mécanismes multilatéraux et bilatéraux.

Recommandations politiques transversales

Normaliser les définitions des images intimes non consensuelles facilitées par l'IA

→ Tirer parti des mécanismes multilatéraux pour prioriser 1) une définition internationale de la violence fondée sur le sexe facilitée par la technologie et de la violence fondée sur le sexe (VFS) qui inclut les IINC facilitées par l'IA et 2) une coopération transfrontalière en matière de réponses juridiques à l'égard des IINC, notamment au sein de l'Organisation des États américains (OEA), en particulier la Commission interaméricaine de la femme (CIM), du processus Beijing+30 d'ONU Femmes et des cadres de gouvernance de l'IA de l'OCDE.

Tirer parti de l'Accord Canada–États-Unis–Mexique pour renforcer la responsabilité des plateformes

→ Proposer une position coordonnée sur la responsabilité des plateformes dans le cadre du prochain examen de l'ACEUM qui s'appuie sur les échecs documentés du chapitre actuel sur le commerce numérique.

- → Étudier les modèles contraignants existants, notamment les obligations d'évaluation des risques prévues par la *Législation sur les services numériques* de l'UE et l'obligation de retrait dans un délai de 48 heures prévu par la loi *TAKE IT DOWN*, comme précédents illustrant à quoi pourraient ressembler concrètement des normes applicables aux plateformes.
- → Parvenir à un accord pour établir des normes de coopération minimale pour les plateformes dans tous les cas d'IINC, y compris des délais de réponse obligatoires aux demandes d'informations émanant des forces de l'ordre et des obligations visant à empêcher la remise en circulation du contenu signalé.
- → Exiger des plateformes qu'elles mettent en œuvre une détection proactive des images d'abus pédosexuels à l'aide de technologies de comparaison des signatures numériques existantes, en tant qu'obligation de base dans les deux pays.

Mettre en place un mécanisme de coopération bilatérale pour les cas transfrontaliers d'images intimes non consensuelles

- → Établir des mécanismes structurés d'échange de connaissances entre les organisations de la société civile, les praticiennes et praticiens du droit et les acteurs institutionnels des deux pays, notamment par le biais de visites d'étude, de programmes de formation conjoints et du partage de documents sur les pratiques efficaces.
- → Officialiser ces échanges par le biais d'accords bilatéraux entre organisations, de mécanismes de financement conjoints ou d'un groupe de travail permanent Canada–Mexique sur les IINC, ainsi que par l'établissement de liens entre les procureures et procureurs des deux pays et le Centre canadien de protection de l'enfance.
- → Mener des projets de recherche bilatéraux afin de mieux documenter les défis liés aux IINC facilitées par l'IA pour favoriser une recherche intersectionnelle et fondée sur le genre.

Combler les lacunes en matière de protection des personnes mineures en misant sur l'éducation

- → Intégrer la littératie numérique et la sécurité en ligne comme éléments essentiels du programme scolaire à tous les niveaux en abordant notamment des sujets comme le consentement, le contenu synthétique, la manipulation numérique, la vie privée et les dynamiques du cyberharcèlement, tout en informant les élèves de leurs droits, des mécanismes de signalement, des conséquences et des services de soutien offerts.
- → Rendre obligatoire l'adaptation des protocoles de prévention de la violence en milieu scolaire afin qu'ils couvrent explicitement les abus par l'image, la violence numérique et le contenu facilité par l'IA, veillant à ce que l'obligation légale qui incombe déjà aux établissements scolaires s'étende à l'environnement numérique.
- → Établir des directives et des outils pratiques normalisés à l'intention des établissements scolaires, par exemple, un manuel axé sur la mise en œuvre qui traduit les politiques en protocoles et procédures applicables en classe.
- → Mettre en œuvre une formation continue qui tient compte des sexospécificités à l'intention des éducatrices et éducateurs, des administratrices et administrateurs, et des élèves. Impliquer tout particulièrement les garçons et les jeunes hommes dans les efforts de prévention afin de remettre en question les normes néfastes et de réduire les actes de violence.

Recommandations particulières pour le Canada

Le cadre juridique canadien comporte les éléments fondamentaux nécessaires pour lutter contre les IINC facilitées par l'IA, mais deux lacunes structurelles compromettent son efficacité : des capacités institutionnelles différentes entre les provinces et des mécanismes de réparation pour les personnes survivantes qui varient considérablement d'une région à l'autre. Les recommandations suivantes visent en priorité à combler ces lacunes.

Renforcer les cadres juridiques

- → Mettre rapidement en place les mesures et politiques nécessaires pour rendre la plus efficace possible la *Loi visant à protéger les victimes* (projet de loi C-16 adopté), notamment en ce qui a trait à la formation des juristes, des corps policiers et des personnes intervenantes auprès des victimes.
- → Prioriser l'adoption du projet de loi C-34 (*Loi sur les médias sociaux sécuritaires*) et veiller à ce qu'il introduise des obligations contraignantes pour les plateformes dans toute future loi fédérale relative aux préjudices en ligne, allant ainsi au-delà des mesures volontaires, comme le marquage numérique et les filtres algorithmiques permettant de détecter les images intimes synthétiques, et afin de mettre en place des mécanismes d'application clairs, comprenant des sanctions importantes en cas de non-conformité.

Améliorer la capacité des institutions pour lutter contre les images intimes non consensuelles facilitées par l'IA

- → Mettre en place un programme de formation interprovincial destiné aux procureures et procureurs de la Couronne, aux services de police et aux juges portant sur les aspects techniques et probants des cas d'IINC facilitées par l'IA, y compris l'informatique judiciaire, la conservation d'éléments de preuve des plateformes en ligne et les décisions judiciaires tenant compte des sexospécificités.
- → S'inspirer des cadres qui existent au Québec et en Colombie-Britannique en tant que modèles établis par des pairs que d'autres provinces peuvent adapter à leurs propres contextes juridiques et institutionnels grâce au partage horizontal des connaissances plutôt qu'à une mise en œuvre du haut vers le bas.
- → Créer un mécanisme fédéral de coordination spécialisé qui met en relation les forces de l'ordre provinciales, les procureures et procureurs de la Couronne, et les organisations de la société civile intervenant dans des cas d'IINC.

Renforcer et normaliser les mécanismes de réparation centrés sur les personnes survivantes

- → Étendre à toutes les provinces le modèle québécois d'ordonnance de cessation et de prévention ou un mécanisme équivalent de retrait d'urgence du contenu afin d'établir une référence nationale pour les mesures de réparation d'urgence qui ne dépend pas du lieu de résidence.
- → En s'inspirant du modèle d'approche d'accompagnement de la Colombie-Britannique, mettre en place un guichet unique national de soutien pour les personnes survivantes des IINC, intégrant des conseils juridiques, une aide au retrait du contenu, un soutien émotionnel et l'aiguillage vers des services locaux.
- → Renforcer l'accès à l'aide juridique pour les cas d'IINC touchant les populations vulnérables et explorer des sources de financement spécifiques pour les organisations de la société civile assurant un accompagnement juridique de première ligne.
- → Mettre en place une initiative nationale de soutien pour les personnes survivantes, accessible à tous les âges, soutenue par du personnel compétent offrant des conseils juridiques, une aide au retrait de contenu et un soutien émotionnel par téléphone et par clavardage. Le site canadien Cybertip.ca offre une base solide, mais son champ d'action est limité aux moins de 18 ans. L'élargissement de son champ d'action pourrait contribuer à combler cette lacune.

Recommandations particulières pour le Mexique

Le défi auquel fait face le Mexique tient moins à une lacune législative qu'à une lacune dans la mise en œuvre. Le cadre de la Ley Olimpia est en vigueur dans l'ensemble des 32 États, mais son efficacité est limitée par des définitions incohérentes, des capacités institutionnelles spécialisées limitées et une procédure de dépôt de plaintes qui place un fardeau disproportionné sur les personnes survivantes. Les recommandations suivantes visent en priorité à combler ces lacunes.

Prioriser la mise en œuvre du cadre juridique existant avant l'adoption de nouvelles lois

- → Réaliser un audit national de l'intégration de la *Ley Olimpia* dans les codes criminels étatiques afin d'identifier les cas où les définitions sont les plus restrictives, où l'application de la loi est la plus faible et où les taux de condamnation sont les plus bas, et utiliser ces constats pour orienter une intervention fédérale ciblée.
- → Créer, à l'échelle nationale, des protocoles de mise en œuvre contraignants pour les cas d'IINC qui normalisent la manière dont les procureures et procureurs classent, enquêtent et montent les cas conformément aux dispositions existantes. Établir des directives claires à l'intention des procureures et procureurs, distinguant la norme en matière de preuve requise pour les atteintes à l'intimité sexuelle de celle requise pour la traite des personnes.
- → Établir des critères techniques, des mécanismes de supervision et des sanctions pour les plateformes numériques, notamment pour prévenir et traiter les IINC facilitées par l'IA.

Renforcer les capacités institutionnelles spécialisées à l'échelle fédérale et étatique

- → Étendre le modèle d'agence spécialisée actuellement en place dans la ville de Mexico et établir des exigences minimales, notamment en matière de capacités de la cyberpolice sur le terrain, de personnel spécialisé et de protocoles tenant compte des sexospécificités.
- → Créer un programme national de formation obligatoire destiné aux procureures et procureurs, aux enquêtrices et enquêteurs, et aux juges portant sur les aspects techniques des cas d'IINC facilitées par l'IA, notamment la conservation des preuves numériques, la chaîne de possession pour le contenu en ligne et les outils probants disponibles pour les cas où les personnes à l'origine des IINC agissent de manière anonyme ou dans plusieurs régions.
- → Établir des protocoles de coopération formels entre les procureures et procureurs et les organisations de la société civile, reconnaissant leur expertise technique et leur soutien aux personnes survivantes comme des atouts institutionnels à part entière.

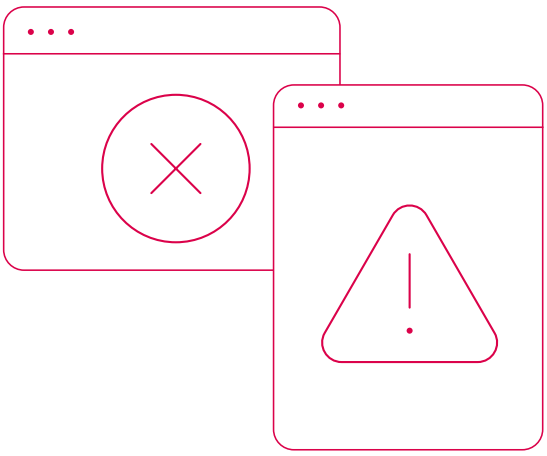
Procéder à une refonte du processus de dépôt de plaintes en privilégiant une approche centrée sur les personnes survivantes

- → Établir un guichet unique national pour signaler les violences numériques qui intègre, au sein d'un mécanisme unique et accessible, le dépôt de plaintes, des conseils en matière de conservation des preuves, des conseils juridiques, un soutien psychologique et de l'aide au retrait du contenu, éliminant ainsi l'obligation actuelle pour les personnes survivantes de s'y retrouver dans des questions juridiques qui varient d'une région à l'autre. Éliminer les pratiques institutionnelles qui constituent des obstacles au signalement, notamment l'obligation pour les personnes survivantes de produire des preuves qui dépassent leurs moyens et les exigences de témoignages répétés devant plusieurs institutions.
- → Mettre en place un système national de collecte de données permettant d'assurer le suivi des plaintes déposées concernant les IINC, du signalement initial jusqu'à la résolution, avec une ventilation notamment par type de contenu, région et résultat. Collaborer avec les principaux groupes de la société civile pour identifier le type de données à recueillir.

CONCLUSION

Les IINC facilitées par l'IA ne sont plus une menace émergente. Elles sont une forme de violence fondée sur le sexe facilitée par la technologie bien ancrée et en croissance qui touche de manière disproportionnée les femmes, les filles et les enfants. Leurs conséquences se font ressentir sur tous les aspects de leur vie, notamment leur sécurité, leur vie privée, leur santé mentale, leurs possibilités économiques et leur capacité à participer pleinement à la vie publique. Partout dans le monde, la technologie continue de devancer les politiques, obligeant les personnes survivantes à se débrouiller au sein de systèmes fragmentés qui n'ont pas été conçus pour les protéger.

Malgré des contextes différents, la comparaison entre le Canada et le Mexique montre que les deux pays font face à des défis structurels semblables : une influence limitée sur les plateformes basées aux États-Unis, des réponses institutionnelles fragmentées et des lacunes persistantes entre la reconnaissance juridique et la mise en œuvre efficace. Le défi principal n'est pas l'absence de législation, mais bien le manque de capacités spécialisées, de processus centrés sur les personnes survivantes et de gouvernance coordonnée nécessaires pour que les protections existantes fonctionnent dans la pratique. Les faits sont clairs. Reste à savoir si les deux pays traiteront cette question avec l'urgence et le sérieux qu'elle exige.



Notes

1. Security Hero (n.d.). *2023 State of deepfakes. Realities, Threats, and Impact*. https://www.securityhero.io/state-of-deepfakes/

2. Conger, K. et coll., (22 janvier 2026). Musk's Chatbot Flooded X With Millions of Sexualized Images in Days, New Estimates Show. *The New York Times*. https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html

3. Vallance, C. (8 janvier 2026). Elon Musk's Grok AI appears to have made child sexual imagery, says charity. *BBC*. https://www.bbc.com/news/articles/cvg1mzlryxeo

4. Fry, D. (10 octobre 2025). Millions of children face sexual violence as AI deepfakes drive surge in new cases – latest global data. *The Conversation*. https://theconversation.com/millions-of-children-face-sexual-violence-as-ai-deepfakes-drive-surge-in-new-cases-latest-global-data-266171

5. UNICEF (2026). '*Deepfake abuse is abuse.*' https://www.unicef.org/lac/en/press-releases/deepfake-abuse-abuse

6. Wong, M. (15 janvier 2026). A Tipping Point in Online Child Abuse. *The Atlantic*. https://www.theatlantic.com/technology/2026/01/ais-child-porn-problem-getting-much-worse/685641/?mc_cid=d15749e2ca&mc_eid=3bc3a71315

7. Affoum, N., Santgostino, I., Vohra, N. & Wodon, Q. (2023). *Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws.* World Bank. https://documents1.worldbank.org/curated/en/099456506262310384/pdf/IDU0c7c3a5a70b56a04b250a31b0b32b8f5cd856.pdf

8. Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., Sharkawy, A. (2025). Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review. *Social Sciences & Humanities Open, 12,* 101882. https://doi.org/10.1016/j.ssaho.2025.101882

9. Kira, B. (3 juin 2024). Deepfakes, the Weaponisation of AI Against Women and Possible Solutions. *Verfassungsblog*. https://verfassungsblog.de/deepfakes-ncid-ai-regulation/

10. Kopecký, K., & Voráč, D. (2026). The phenomenon of deep nudes—a new threat to children and adults. *AI & Society,* 41, 545–556. https://doi.org/10.1007/s00146-025-02425-4

11. Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., Sharkawy, A. (2025). Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review. *Social Sciences & Humanities Open, 12,* 101882. https://doi.org/10.1016/j.ssaho.2025.101882

12. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

13. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich- Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

14. Kristof, N. (16 avril 2021). Why Do We Let Corporations Profit From Rape Videos? *The New York Times*. https://www.nytimes.com/2021/04/16/opinion/sunday/companies-online-rape-videos.html?smid=tw-share

15.Tech Transparency Project (27 janvier 2026). *Nudify Apps Widely Available in Apple and Google App Stores*. https://www.techtransparencyproject.org/articles/nudify-apps-widely-available-in-apple-and-google-app-stores

16. Mantzarlis, A. & Lakatos, S. (14 juillet 2025). AI Nudifiers continue to reach millions and make millions. *Indicator.* https://indicator.media/p/ai-nudifiers-continue-to-reach-millions-and-make-millions

17. AI Security Institute (2026). *International AI Safety Report 2026*. https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

18. Department for Science, Innovation and Technology (2025). *New law to tackle AI child abuse images at source as reports more than double.* Gouvernement du Royaume-Uni. https://www.gov.uk/government/news/new-law-to-tackle-ai-child-abuse-images-at-source-as-reports-more-than-double

19. D'Anastasio, C. (15 septembre 2025). AI is replacing online moderators, but it's bad at the job. *The Star*. https://www.thestar.com.my/tech/tech-news/2025/09/15/ai-is-replacing-online-moderators-but-it039s-bad-at-the-job#goog_rewarded

20. Priyam, P. (11 mars 2026). *Why AI Content Moderation Keeps Getting It Wrong — And a Framework to Fix.* LinkedIn. https://www.linkedin.com/pulse/why-ai-content-moderation-keeps-getting-wrong-framework-prachi-priyam-yhwuc/

21. Cette information a été fournie par les expertes et experts interrogés dans le cadre de ce rapport. Consultez les remerciements pour en savoir plus sur les personnes interviewées.

22. Pour plus d'informations, consultez : http://stopncii.org

23. Pour plus d'informations, consultez : https://takeitdown.ncmec.org/

24. Meta. (12 juin 2025). *Taking Action Against 'Nudify' Apps.* https://about.fb.com/news/2025/06/taking-action-against-nudify-apps/

25. Swiss Info (18 janvier 2025). El fundador de Telegram reconoció la «gravedad» de los hechos que le imputa la justicia francesa. *SWI swissinfo.ch.* https://www.swissinfo.ch/spa/el-fundador-de-telegram-reconoci%C3%B3-la-%22gravedad%22-de-los-hechos-que-le-imputa-la-justicia-francesa/88743834

26. Chiu, D. (2 juin 2025). *City Attorney shuts down 10 websites that create nonconsensual deepfake pornography.* Ville et comté de San Francisco. https://www.sf.gov/news-city-attorney-shuts-down-10-websites-that-create-nonconsensual-deepfake-pornography

27. Robins-Early, N. (24 mars 2026). Baltimore sues Elon Musk's AI company over Grok's fake nude images. *The Guardian.* https://www.theguardian.com/technology/2026/mar/24/elon-musk-grok-ai-lawsuit-baltimore

28. Haeck, P. (26 mars 2026). Dutch court bans Grok from generating fake nudes, threatens €100K daily penalties. *Politico*. https://www.politico.eu/article/netherlands-grok-x-ban-generative-pictures-penalties/

29. McQue, K. (24 mars 2026). Meta ordered to pay $375m after being found liable in child exploitation case. *The Guardian*. https://www.theguardian.com/technology/2026/mar/24/meta-new-mexico-jury

30. Commission européenne (6 mai 2026). *L'UE convient de simplifier les règles en matière d'IA afin de stimuler l'innovation et d'interdire les applications de « déshabillage » (« nudification ») pour protéger les citoyens.* https://ec.europa.eu/commission/presscorner/detail/fr/ip_26_1024

31. Affoum, N., Santgostino, I., Vohra, N. & Wodon, Q. (2023). *Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws.* World Bank. https://documents1.worldbank.org/curated/en/099456506262310384/pdf/IDU0c7c3a5a70b56a04b250a31b0b32b8f5cd856.pdf

32. Carmo, A. (25 novembre 2025). AI and anonymity fuel surge in digital violence against women. *United Nations News.* https://news.un.org/en/story/2025/11/1166411

33. Griffiths, O. (2024). Criminal Code Amendment (Deepfake Sexual Material) Bill 2024. *Bills Digest No. 81, 2023-24.* Parliament de l'Australie. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2324a/24bd081

34. Schriever, J. (26 février 2026). Deepfakes back in the headlines after a federal law was used for the first time. Australian Broadcasting Corporation. https://www.abc.net.au/news/2026-02-27/rise-in-sexualised-deepfakes-new-laws-explainer/106390940

35. Gobierno de Canadá (2026, 18 de junio). *Protecting Victims Act: Legislation to protect victims and keep kids safe from predators.* https://www.justice.gc.ca/eng/csj-sjc/pl/c16/index.html

63. Karttunen, S. (2026). *The Danish approach to copyright and deepfakes: A model for the EU?* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf

37. Carter, H. (17 septembre 2025). South Korea's Act on Special Cases with Respect to Punishing Sex Crimes. *Facia.* https://facia.ai/knowledgebase/south-koreas-act-on-special-cases-with-respect-to-punishing-sex-crimes/

38. Barr, H. (29 août 2024). South Korea's Digital Sex Crime Deepfake Crisis. *Human Rights Watch.* https://www.hrw.org/news/2024/08/29/south-koreas-digital-sex-crime-deepfake-crisis

39. Information Commissioner's Office. (2025). T*he Data Use and Access Act 2025 (DUAA) – what does it mean for organisations?* https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/

40. UN Women, & Sexual Violence Research Initiative. (2025). *Global trends to prevent and respond to technology-facilitated violence against women and girls: A compendium of emerging practices*. https://www.unwomen.org/sites/default/files/2025-12/global-trends-to-prevent-and-respond-to-technology-facilitated-violence-against-women-and-girls-en_1.pdf

41. International Centre for Missing & Exploited Children. (2023). *Child Sexual Abuse Material: Model Legislation & Global Review.* https://cdn.icmec.org/wp-content/uploads/2023/10/CSAM-Model-Legislation_10th-Ed-Oct-2023.pdf

42. Kuo, V., & Raidma, G. (2024). *Global CSAM Legislative Overview.* INHOPE. https://inhope.org/media/pages/articles/global-csam-legislative-overview-2024/71acaa8826-1765986997/executive-summary-global-csam-legislative-overview-2024.pdf

43. Protect Children. (2026). *CSAM Perpetrator Research Report: Findings from a Survey of CSAM Perpetrators on Digital Platform Use and Design (Tell Me More About Tech).* Ofcom. https://www.protectchildren.fi/en/post/tmat-csam-perpetrator-research-report

44. Leblond, P. (2022). *The USMCA and digital trade in North America*. The Brookings Institution. https://www.brookings.edu/articles/usmca-forward-building-a-more-competitive-inclusive-and-sustainable-north-american-economy-digital/

45. Vargas-Chaves, I. (2025). Take it Down Act: un análisis crítico de su rol contra la difusión no consentida de imágenes y deepfakes. *Revista Criminalidad, 67*(3), 39-55. https://doi.org/10.47741/17943108.729

46. Congrès des États-Unis. (19 mai 2025). *TAKE IT DOWN Act (S.146, 119th Congress)*. https://www.congress.gov/bill/119th-congress/senate-bill/146/text

47. Congrès des États-Unis. (21 mai 2025). *DEFIANCE Act of 2025 (H.R. 3562, 119th Congress).* https://www.congress.gov/bill/119th-congress/house-bill/3562

48. Mithani, J. (13 janvier 2026). Senate moves to let victims of sexually explicit deepfakes sue for damages. *The 19th.* https://19thnews.org/2026/01/senate-defiance-act-nonconsensual-images-deepfakes/

49. Aguirre-Lanegra, A., & Ramos, F. (2025). Deepfakes sexuales y violencia algorítmica: hacia un marco normativo integral de protección de la dignidad digital. *Estudios En Derecho a La Información, 11*(21), e20198. https://doi.org/10.22201/iij.25940082e.2026.21.20198

50. Congrès des États-Unis. (26 juin 2025). *STOP CSAM Act of 2025 (S.1829, 119th Congress).* https://www.congress.gov/bill/119th-congress/senate-bill/1829/text

51. Bowman, T. (13 juin 2025). The STOP CSAM Act Would Make Kids Less Safe. *Center for Democracy & Technology.* https://cdt.org/insights/the-stop-csam-act-would-make-kids-less-safe/

52. Pour plus d'informations, consultez : https://takeitdown.ncmec.org/

53. Pour plus d'informations, consultez : https://www.missingkids.org/gethelpnow/cybertipline

54. Avendaño, E., Contreras, A., Macías, G., Paéz, S., Rivera, K., Samperí, A., Soria, E., & Valerio, S. (2025). *Una mirada crítica feminista al delito de difusión de contenido íntimo sin consentimiento.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2025/03/InformeJuridico_Luchadoras_1.pdf

55. Defend Dignity. (2024). *Submission to the Standing Committee on Canadian Heritage. Study: Harms Caused to Children, Women, and Men by the Ease of Access to, and Online Viewing of, Illegal Sexually Explicit Material.* https://www.ourcommons.ca/Content/Committee/441/CHPC/Brief/BR13053693/br-external/DefendDignity-e.pdf

56. Mortimer, S., Phippen, A., & Wright, D. (12 mars 2025). The Scale of Non-Consensual Intimate Image (NCII) Abuse: A Data-Driven Global Analysis. *South West Grid for Learning.* https://swgfl.org.uk/magazine/the-scale-of-non-consensual-intimate-image-ncii-abuse-a-data-driven-global-analysis/

57. Serebin, J. (26 avril 2023). Quebec man who created synthetic, AI-generated child pornography sentenced to prison. *CBC News.* https://www.cbc.ca/news/canada/montreal/ai-child-abuse-images-1.6823808

58. Bernhardt, D. (15 décembre 2023). AI-generated fake nude photos of girls from Winnipeg school posted online. *CBC News.* https://www.cbc.ca/news/canada/manitoba/artificial-intelligence-nude-doctored-photos-students-high-school-winnipeg-1.7060569

59. Pour plus d'informations, consultez : https://cybertip.ca/fr/

60. Rosen, K. (16 février 2024). No charges laid over explicit, AI-generated photos of Winnipeg students. *CTV News.* https://www.ctvnews.ca/winnipeg/article/no-charges-laid-over-explicit-ai-generated-photos-of-winnipeg-students/

61. Dubinski, K. (4 avril 2024). Kids call for more lessons on AI after fake nudes posted by London Catholic students. *CBC News.* https://www.cbc.ca/news/canada/london/london-ontario-st-thomas-aquinas-sta-deepfake-ai-nude-sexual-imagery-1.7163183

62. Dubinski, K. (25 avril 2024). No charges against Catholic high school students who made and shared deep-fake nudes of classmates. *CBC News.* https://www.cbc.ca/news/canada/london/st-thomas-aquinas-nude-photos-artificial-intelligence-1.7183878

63. Gouvernement du Canada (18 juin 2026). *Modifications aux peines dans le projet de loi C-16.* https://www.justice.gc.ca/fra/sjc-csj/pl/c16/mpp-pcs.html

64. Gouvernement du Canada (18 juin 2026). *Modifications aux peines dans le projet de loi C-16*. https://www.justice.gc.ca/fra/sjc-csj/pl/c16/mpp-pcs.html

65. Gouvernement du Canada (10 juin 2026). *Government of Canada introduces legislation to make social media services and AI chatbots safer for children.* https://www.canada.ca/en/canadian-heritage/news/2026/06/government-of-canada-introduces-legislation-to-make-social-media-services-and-ai-chatbots-safer-for-children.html

66. Gouvernement du Canada (10 juin 2026). *Bill C-34, the Safe Social Media Act.* https://www.canada.ca/en/canadian-heritage/services/safe-social-media-act.html

67. Commissariat à la protection de la vie privée du Canada. (15 janvier 2026). *Le Commissaire à la protection de la vie privée du Canada élargit son enquête sur la plateforme de média social X à la suite de reportages signalant des images hypertruquées à caractère sexuel générées par l'IA*. https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2026/nr-c_260115/

68. Djuric, M. (15 janvier 2026). Canada's privacy watchdog investigating Musk's xAI over sexualized deepfakes. *Politico.* https://www.politico.com/news/2026/01/15/canadas-privacy-watchdog-investigating-musks-xai-over-sexualized-deepfakes-00731587

69. Gouvernement du Québec. (2024). *Loi visant à contrer le partage sans consentement d'images intimes,* CQLR c. P-9.0002. https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-9.0002

70. Gouvernement de la Colombie-Britannique. (2026). *Intimate Images Protection Act*. https://www2.gov.bc.ca/gov/content/safety/public-safety/intimate-images/intimate-images-consent

71. Assemblée législative du Nouveau-Brunswick. (2022). *Loi sur la communication illégale d'images intimes*, LN-B 2022, c. 1. https://www.canlii.org/fr/nb/legis/lois/ln-b-2022-c-1/215517/ln-b-2022-c-1.html

72. Gouvernement de l'Île-du-Prince-Édouard. (2021). *Intimate Images Protection Act,* RSPEI 1988, c. I-9.1. https://canlii.ca/t/54w8w

73. Pour plus d'informations, consultez : https://www.cyberscan.io/en/

74. Salamis, B. (2025). *Stolen Faces: Policy Options to Mitigate Harm from Non-Consensual AI-Generated Intimate Image Abuse in Canada*. Simon Fraser University. https://summit.sfu.ca/_flysystem/fedora/2025-06/etd23790.pdf

75. Lyon, J. (1976). The Central Fallacy of Canadian Constitutional Law. *McGill Law Journal,* 22(1). https://lawjournal.mcgill.ca/article/the-central-fallacy-of-canadian-constitutional-law/

76. Gouvernement du Québec. (n.d.). Partage sans consentement d'une image intime. https://www.quebec.ca/justice-et-etat-civil/accompagnement-victimes-crime/partage-sans-consentement-image-intime

77. McKenzie, T. & Kerr, L. (2024). *Quebec B.C.'s New Intimate Images Protection Act.* BarTalk. https://www.bartalk.org/article/the-law/b-c-s-new-intimate-images-protection-act

78. Pour plus d'informations, consultez : https://novascotia.ca/cyberscan/fr/

79. Irwin, J, Dharamshi, A., Zon, N. (2021). *Children's Privacy in the Age of Artificial Intelligence*. Canadian Standards Association. https://www.csagroup.org/article/research/childrens-privacy-in-the-age-of-artificial-intelligence/?srsltid=AfmBOorVdFE_TMOCF-f0bVKRyGJQNflySTj8bOYfgxzAD20IgTAHAgdK

80. Siekierski, B. (2019). Hypertrucage : Que peut-on faire à propos du contenu audio et vidéo de synthèse? *Service d'information et de recherche parlementaires. Publication no 2019-11-F.* https://publications.gc.ca/collections/collection_2019/bdp-lop/eb/YM32-5-2019-11-fra.pdf

81. Salamis, B. (2025). *Stolen Faces: Policy Options to Mitigate Harm from Non-Consensual AI-Generated Intimate Image Abuse in Canada.* Simon Fraser University. https://summit.sfu.ca/_flysystem/fedora/2025-06/etd23790.pdf

82. Aguirre, I., Barrera, L., Zamora, A., Rangel, Y. (2020). *Justicia en trámite. El limbo de las investigaciones sobre violencia digital en México.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2024/10/Luchadoras_JusticiaEnTramite.pdf

83. Instituto Nacional de Estadística y Geografía. (2025). *Módulo sobre Ciberacoso (MOCIBA) 2024.* https://www.inegi.org.mx/contenidos/programas/mociba/2024/doc/mociba2024_resultados.pdf

84. ONU Mujeres. (2025). *Violencia digital contra las mujeres y las niñas*. https://mexico.unwomen.org/sites/default/files/2025-12/onu_mujeres_mexico_brief_violencia_digital_101125.pdf

85. ONU Mujeres. (2025). *Violencia digital contra las mujeres y las niñas.* https://mexico.unwomen.org/sites/default/files/2025-12/onu_mujeres_mexico_brief_violencia_digital_101125.pdf

86. Burgess, M. (14 juillet 2025). Esas aplicaciones que "desnudan" gente con IA están generando 36 millones de dólares al año. *Wired.* https://es.wired.com/articulos/esas-aplicaciones-que-desnudan-gente-con-ia-estan-generando-36-millones-de-dolares-al-ano

87. EFE. (24 janvier 2024). Ciudad Juárez, primer lugar en producción de videos sobre abuso sexual infantil. *El Financiero.* https://www.elfinanciero.com.mx/nacional/2024/01/24/ciudad-juarez-primer-lugar-en-produccion-de-videos-sobre-abuso-sexual-infantil/

88. EFE. (16 juillet 2025). Trata por material de abuso de menores en México sube 86 % en primer trimestre 2025. *SWI swissinfo.ch.* https://www.swissinfo.ch/spa/trata-por-material-de-abuso-de-menores-en-m%C3%A9xico-sube-86-%25-en-primer-trimestre-2025/89686591

89. Rodríguez. A. (23 mai 2025). Sentenciado a cinco años de prisión Diego N, ex alumno del IPN, por el delito de pornografía infantil. *El País.* https://elpais.com/mexico/2025-05-23/sentenciado-a-cinco-anos-de-prision-diego-n-ex-alumno-del-ipn-por-el-delito-de-pornografia-infantil.html

90. Rodríguez, A. (11 novembre 2025). Al menos 400 alumnas de secundaria denuncian la alteración de sus fotos con IA para fines pornográficos en Zacatecas. *El País.* https://elpais.com/mexico/2025-11-11/al-menos-400-alumnas-de-secundaria-denuncian-la-alteracion-de-sus-fotos-con-ia-para-fines-pornograficos-en-zacatecas.html

91. Orden Jurídico de México. (n.d). *Ficha técnica Ley Olimpia.* https://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

92. Escobar, C. & Trujano, M. (25 avril 2023). Sentencias por "Ley Olimpia", en 1% de los casos investigados. *Serendipia.* https://serendipia.digital/violencia-contra-las-mujeres/sentencias-por-ley-olimpia/

93. Cámara de Diputados del H. Congreso de la Unión. (11 février 2007). *Ley general de acceso de las mujeres a una vida libre de violencia.* Dernier amendement 15 janvier 2026. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

94. Cámara de Diputados del H. Congreso de la Unión. (1er juin 2021). *Código penal federal.* https://www.diputados.gob.mx/LeyesBiblio/ref/cpf/CPF_ref150_01jun21.pdf

95. Cámara de Diputados del H. Congreso de la Unión. (14 juin 2012). *Ley general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos.* Dernière modification publiée DOF 19-01-2018 https://www.gob.mx/indesol/documentos/ley-general-para-prevenir-sancionar-y-erradicar-los-delitos-en-materia-de-trata-de-personas-y

96. Avendaño, E., Contreras, A., Macías, G., Paéz, S., Rivera, K., Samperí, A., Soria, E., & Valerio, S. (2025). *Una mirada crítica feminista al delito de difusión de contenido íntimo sin consentimiento.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2025/03/InformeJuridico_Luchadoras_1.pdf

97. Te protejo México, (n.d.) *Marco legislativo del material de abuso sexual infantil federal y estatal de México.* https://teprotejomexico.org/wp-content/uploads/sites/2/2025/02/marco-legislativo-tpm.pdf

98. Te protejo México, (n.d.) *Marco legislativo del material de abuso sexual infantil federal y estatal de México.* https://teprotejomexico.org/wp-content/uploads/sites/2/2025/02/marco-legislativo-tpm.pdf

99. Suprema Corte de Justicia de la Nación. (2023). *Protocolo para juzgar con perspectiva de género.* https://www.scjn.gob.mx/derechos-humanos/sites/default/files/protocolos/archivos/2020-11/Protocolo%20para%20juzgar%20con%20perspectiva%20de%20g%C3%A9nero%20%28191120%29.pdf

100. Samperí, A., Contreras, A., Avendaño, E., Soria, E., Macías, G., Rivera, K., Paéz, S., & Valerio, S. (2025). *Una mirada crítica feminista al delito de difusión de contenido íntimo sin consentimiento.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2025/03/InformeJuridico_Luchadoras_1.pdf

101. Cámara de Diputados del H. Congreso de la Unión. (26 mai, 14 juillet, 31 août 1928). *Código Civil Federal.* DOF 14-11-2025. https://mexico.justia.com/federales/codigos/codigo-civil-federal/

102. Secretaría de las Mujeres de la Ciudad de México. (n.d.). *Violencia digital.* https://semujeres.cdmx.gob.mx/violencia-digital

103. Gobierno de la Ciudad de México. (n.d.). *Línea Mujeres.* https://cms311.cdmx.gob.mx/linea-mujeres/

104. Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes. (n.d.). *SIPINNA Estado de México.* https://sipinna.edomex.gob.mx/sipinna_nacional

105. Pour plus d'informations, consultez : https://cultivandogeneroac.org/

106. Pour plus d'informations, consultez : https://defensorasdigitales.org/

107. Pour plus d'informations, consultez : https://hijasdeinternet.org/

108. Pour plus d'informations, consultez : https://luchadoras.mx/

109. Pour plus d'informations, consultez : https://socialtic.org/

110. Escobar, C. & Trujano, M. (23 avril 2023). Sentencias por "Ley Olimpia", en 1% de los casos investigados. *Serendipia.* https://serendipia.digital/violencia-contra-las-mujeres/sentencias-por-ley-olimpia/

111. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

112. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

113. Cámara de Diputados del H. Congreso de la Unión. (30 septembre 2019). *Ley general de educación.* Dernière modification publié DOF 15-01-2026 https://www.diputados.gob.mx/LeyesBiblio/pdf/LGE.pdf

Utilisation de l'IA : des outils d'intelligence artificielle ont été utilisés uniquement à des fins rédactionnelles, pour la révision linguistique et la reformulation.



IVADO

EON INSTITUTE

avec le soutien de

CANADA FIRST RESEARCH EXCELLENCE FUND

APOGÉE CANADA FONDS D'EXCELLENCE EN RECHERCHE