Cerrando las brechas: **Abordando el problema de las imágenes íntimas no consentidas facilitadas por IA en Canadá y México.** Un análisis comparativo.

Autoras: **Daniela Rojas** y **Claudia Del Pozo**
Contribuidoras: **Nicté Cabañas y Amélie Côté**

Octubre 2026



IVADO
EON INSTITUTE

con el apoyo de

CANADA FIRST RESEARCH EXCELLENCE FUND
APOGÉE CANADA FONDS D'EXCELLENCE EN RECHERCHE

Agradecimientos

Las autoras expresan su más sincero agradecimiento a todas las personas que contribuyeron a este proyecto como participantes en las entrevistas de ambos países. Apreciamos profundamente el tiempo y los valiosos conocimientos de las personas participantes, los cuales fueron claves en la elaboración de este informe. Sus nombres se encuentran a continuación en orden alfabético.

Elizabeth Avendaño, abogada y activista feminista en Luchadoras

Senator Luis Donaldo Colosio, presidente de la Comisión de Derechos Digitales del Senado de la República de México

Sarah Crawford, directora ejecutiva del Centro Canadiense de Recursos para Víctimas de Delitos

Elise Dupras, especialista en intervención en materia de delincuencia juvenil y asesora de ciberacoso escolar en el Consejo Escolar Marguerite-Bourgeoys

Marcela Hernández, cofundadora de Defensora Digitales

Floretta Mayerson, cofundadora de Violetta

Paola Ricaurte Quijano, profesora investigadora del Tecnológico de Monterrey

Catherine Régis, profesora titular en la Universidad de Montreal

Teresa Scassa, profesora investigadora de la Universidad de Ottawa.

Las afirmaciones contenidas en el informe no reflejan necesariamente las opiniones de las expertas y del experto consultados, sino que corresponden únicamente a las autoras del informe.

Este documento ha sido posible gracias a la colaboración entre Eon Institute en México e IVADO en Canadá. Eon Institute es un think tank mexicano que trabaja en América Latina para impulsar sociedades más resilientes en la era de la IA a través de investigación aplicada, formación y articulación, conectando evidencia y actores para desarrollar mejores políticas y estrategias. IVADO es un consorcio interdisciplinario e intersectorial de investigación y movilización del conocimiento liderado por la Universidad de Montreal, cuya misión es desarrollar y promover una IA sólida, racional y responsable.

ÍNDICE

03 **Aprendizajes Clave**

04 **Introducción**

05 **Impactos individuales y sociales de las imágenes íntimas no consentidas facilitadas por IA**

05 **El papel de las empresas tecnológicas en la cadena de daño de las imágenes íntimas no consentidas facilitadas por IA**

07 **Panorama general de los marcos regulatorios y las políticas públicas en el mundo**

07 Principales tendencias en la regulación de las imágenes íntimas no consentidas facilitadas por IA

10 Tendencias comunes en la regulación del material de abuso sexual infantil

10 Estados Unidos: La ley TAKE IT DOWN y más allá

12 **Perfil de país: Canadá**

12 Panorama del abuso de las imágenes íntimas no consentidas facilitadas por IA en Canadá

13 Marco regulatorio

14 Mecanismos de denuncia y reparación

15 Vacíos regulatorios, implementación y coordinación

16 **Perfil de país: México**

16 Panorama del abuso con imágenes íntimas no consentidas facilitadas por IA en México

16 Marco regulatorio

17 Mecanismos de denuncia y reparación

18 Vacíos regulatorios, de implementación y coordinación

19 **Hallazgos comparativos clave**

21 **Recomendaciones de política pública**

21 Recomendaciones de política pública transversales

22 Recomendaciones específicas para Canadá

23 Recomendaciones específicas para México

24 **Conclusión**

25 **Notas**

APRENDIZAJES CLAVE

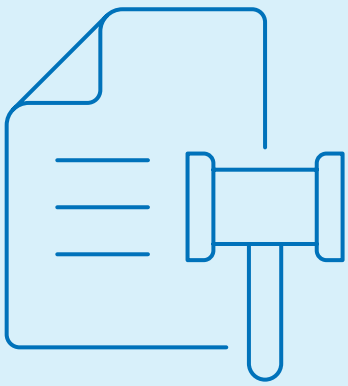
Este reporte analiza cómo Canadá y México están respondiendo ante las imágenes íntimas no consentidas (NCII, por sus siglas en inglés) facilitadas por IA, al identificar brechas en la prevención, reparación y rendición de cuentas. A pesar de regirse por tradiciones jurídicas y contextos institucionales muy diferentes, ambos países se enfrentan a los mismos problemas de fondo.

Lo que se descubrió

- Existen marcos legales, pero estos no se traducen en justicia. En México, únicamente el 0.5% de las denuncias por NCII llegan a juicio. En Canadá, la protección varía considerablemente según la provincia en la que resida la persona sobreviviente, aunque las protecciones del Código Penal fueron reforzadas en Junio de 2026, por lo que será necesario analizar con mayor detenimiento cómo se implementan.
- La capacidad institucional es el principal cuello de botella. Fiscales, jueces y agentes del orden público carecen tanto de entrenamiento técnico, como de la perspectiva de género necesaria para investigar y sancionar de forma efectiva estos casos.
- Las plataformas digitales operan sin obligaciones de carácter vinculante. Introducido en junio de 2026, el proyecto de ley canadiense C-34 tiene como objetivo de imponer nuevas obligaciones reglamentarias. En octubre de 2026, México reforzó la protección de los menores, sin precisar las modalidades de aplicación ni establecer sanciones. Sin embargo, la mayoría tienen su sede en Estados Unidos y el capítulo de servicios digitales del Tratado entre México, Estados Unidos y Canadá (T-MEC) limita la capacidad de los gobiernos de Canadá y México para exigirles rendición de cuentas.
- Las personas más afectadas (comunidades indígenas, mujeres racializadas y menores) son aquellas que tienen menos acceso a la justicia debido a barreras agravantes.

Lo que se recomienda

- Para ambos países: coordinar una postura conjunta de cara a la próxima revisión del T-MEC con el fin de establecer estándares mínimos de rendición de cuentas.
- Para Canadá: priorizar la implementación de las nuevas medidas propuestas en el marco de la *Protecting Victims Act* (Ley de Protección a las Víctimas) o Proyecto de Ley C-16 (aprobado en junio de 2026); prioriza la aprobación del Proyecto de Ley C-34, *Safe Social Media Act* (Ley de Seguridad en las Redes Sociales), presentado en junio de 2026; y ampliar los mecanismos de reparación de emergencia a todas las provincias.
- Para México: enfocarse en la implementación de la existente Ley Olimpia antes de perseguir una nueva legislación y desarrollar protocolos nacionales para fiscales y una vía única de denuncia para las personas sobrevivientes.



INTRODUCCIÓN

El despliegue reciente y amplio de las herramientas de inteligencia artificial (IA) no ha generado la violencia digital por razón de género, pero la ha transformado fundamentalmente. La IA generativa ha reducido las barreras de producción y de difusión de imágenes íntimas no consentidas (NCII, por sus siglas en inglés), ya que se requieren unas habilidades técnicas mínimas por parte de las personas perpetradoras y el costo es bajo, además de reducir el riesgo de rendición de cuentas. En última instancia, esto alimenta una forma más rápida y accesible de violencia de género facilitada por la tecnología.

La magnitud del fenómeno es impactante. En 2023, el 98% de los videos *deepfake* o ultrafalsos se realizaron sin consentimiento, y el 99% de estos representaban a mujeres.[1] El caso de Grok (el modelo de lenguaje de gran tamaño de X) ilustra este fenómeno: a inicios de 2026, se utilizó para generar aproximadamente 1.8 millones de imágenes sexualizadas de mujeres en solo nueve días,[2] lo que corresponde a dos imágenes por cada segundo. Esta violencia no se limita a las personas adultas. El mismo caso reveló material de abuso sexual infantil (CSAM, por sus siglas en inglés) involucrando a niñas de entre 11 y 13 años.[3] De hecho, las denuncias de CSAM facilitado por IA aumentaron un 1,325% entre 2023 y 2024,[4] con un estudio de 2025 que se realizó en once países y que indica que al menos 1.2 millones de imágenes de niños y niñas fueron manipuladas para crear ultrafalsos sexuales explícitos.[5] Además, la Internet Watch Foundation (IWF) reportó 3,440 videos de CSAM facilitados por IA en 2025, en contraste con los 13 del año anterior.[6]

A pesar de la creciente evidencia de las consecuencias emocionales, económicas, sociales y democráticas de las NCII facilitadas por IA, las respuestas de política pública siguen siendo insuficientes. En 2023, solo un tercio de las economías tenían leyes de protección contra el acoso cibernético, entre ellos Canadá y México,[7] e incluso cuando existe dicha legislación su aplicación es débil.

Canadá y México ofrecen una perspectiva comparativa particularmente ilustrativa. Ambos países navegan por las complejidades de los sistemas federales, mientras lidian con las plataformas basadas en EE. UU. que, en gran medida, quedan fuera de su ámbito regulatorio. Además, cuentan con una capacidad limitada para hacer cumplir la ley, y los fondos para los sistemas de apoyo a las personas sobrevivientes son insuficientes. Este informe analiza cómo Canadá y México están respondiendo a las NCII facilitadas por IA, al identificar brechas estructurales en la prevención, reparación y rendición de cuentas en ambos contextos y proponiendo recomendaciones de política pública concretas a las personas formuladoras de política pública de ambos países.

Limitaciones en la metodología

La metodología para este informe se basa en un enfoque cualitativo, comparativo e interdisciplinar que combina un análisis documental, incluidos marcos normativos, sentencias jurídicas, informes de la sociedad civil y literatura académica, con nueve entrevistas semiestructuradas realizadas entre febrero y marzo de 2026 a personas expertas de la sociedad civil, academia, práctica jurídica e instituciones públicas de ambos países. La selección de las personas entrevistadas se realizó de manera intencionada, pero la muestra no es exhaustiva en ninguno de los dos ecosistemas. Aunque la muestra canadiense no incluye una voz legislativa, unas de las personas entrevistadas han participado directamente en cuestiones legislativas a través de investigaciones, contribuciones a informes oficiales y colaboraciones en políticas públicas.

IMPACTOS INDIVIDUALES Y SOCIALES DE LAS IMÁGENES ÍNTIMAS NO CONSENTIDAS FACILITADAS POR IA

Los espacios digitales se han convertido en un escenario central para la violencia por razón de género. Estos espacios no son solo una extensión del daño fuera del ámbito digital, sino que funcionan como ecosistemas con sus propias dinámicas, herramientas y estructuras de poder, donde las formas tradicionales de violencia encuentran nuevos instrumentos.

Una idea errónea que influye en las respuestas institucionales es que la naturaleza sintética de las NCII facilitadas por IA causa menos daños. La evidencia sugiere lo contrario; las personas sobrevivientes experimentan estrés crónico, ansiedad, depresión y pérdida de la autoestima, y algunas víctimas se suicidan,[8] lo cual es comparable a lo que experimentan las personas sobrevivientes de NCII no sintéticas.[9] Estas consecuencias se extienden a la vida profesional y académica, dañando la reputación y afectando la asistencia, la concentración y el desarrollo académico.[10] Las personas sobrevivientes suelen carecer de recursos legales o técnicos accesibles para limitar el daño.

La dimensión de género de este daño va más allá de lo individual y tiene consecuencias sociales más amplias. Al actuar como una forma de control sistemática, la normalización de las NCII facilitadas por IA refuerza la cosificación de las mujeres, intensifica el acoso y desanima su participación pública.[11] Cuando se utiliza en contra de las mujeres en política, periodistas, activistas y candidatas, el contenido sexualizado sintético puede volverse una herramienta de violencia política, que silencia voces, socava su credibilidad y desalienta su liderazgo.[12] Por ejemplo, en las elecciones de México en 2024, 217 mujeres retiraron sus candidaturas debido a la presión, las amenazas o la coerción, mientras que las denuncias formales siguen siendo escasas debido a la intimidación y a la falta de conocimiento de los mecanismos de denuncia.[13]

Es importante señalar que estos daños no son consecuencias inevitables del progreso tecnológico. Estas son las consecuencias de decisiones específicas en el diseño, de lagunas normativas, de limitaciones institucionales y de la insuficiente rendición de cuentas por parte de las empresas tecnológicas.

EL PAPEL DE LAS EMPRESAS TECNOLÓGICAS EN LA CADENA DE DAÑO DE LAS IMÁGENES ÍNTIMAS NO CONSENTIDAS FACILITADAS POR IA

El daño causado por las NCII facilitadas por IA surge de un ecosistema de actores interconectados que operan a diferentes niveles de la cadena de daño. A nivel de creación, se encuentran tanto las aplicaciones de desnudez con IA, como las plataformas de IA generativa que se utilizan indebidamente y a nivel de amplificación están las redes sociales y las plataformas de contenido donde se desarrolla y se amplifica la violencia. A continuación, el gráfico 1 ilustra las diferentes etapas de la cadena de daño.

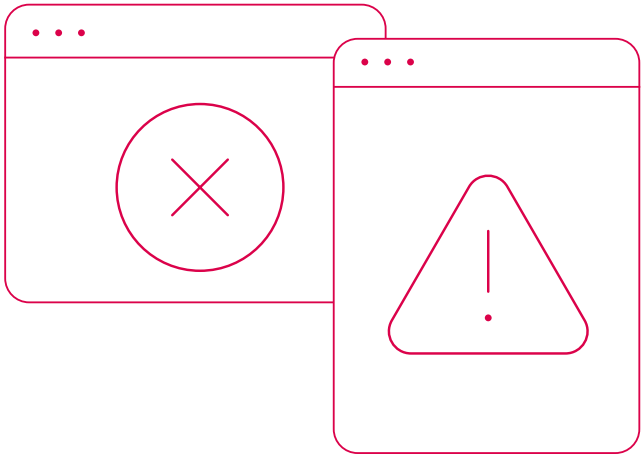


Gráfico 1: Cadena de daño de las NCII facilitadas por IA.



A nivel de creación, muchas plataformas—conocidas como aplicaciones de desnudez con IA— están diseñadas explícitamente para producir y almacenar NCII.[14] Éstas se han convertido en un negocio muy rentable. El Tech Transparency Project evaluó en enero de 2026 el mercado en aproximadamente 117 millones de dólares estadounidenses y 705 millones de descargas de las aplicaciones de desnudez con IA. Muchas de ellas utilizan la infraestructura y los servicios que ofrecen las principales empresas tecnológicas.[15] Dos de los principales proveedores de servicios en la nube proporcionan la infraestructura de alojamiento y distribución de contenidos para 62 de los 85 sitios web de desnudez.[16] Las plataformas de IA generativa también presentan desafíos, ya que pueden ser utilizadas de forma indebida para crear NCII y CSAM, un riesgo que los desarrolladores no pueden probar directamente debido a la ilegalidad del tratamiento de este último tipo de materiales.[17] En respuesta, el Reino Unido autorizó a un número limitado de organizaciones acreditadas a probar modelos de IA bajo condiciones estrictas.[18]

A nivel de amplificación, las redes sociales y las plataformas de contenido establecen las reglas que rigen la moderación de contenido y su cumplimiento. Muchas de estas plataformas utilizan sistemas de IA para detectar violaciones en tiempo real, pero el problema no solo radica en que la moderación de contenidos falle, con una tasa de error que alcanza un 70–80%,[19] sino que los moderadores humanos reciben etiquetas o alertas sin contexto suficiente para actuar de forma adecuada.[20] Además, las personas sobrevivientes reportan respuestas insuficientes por parte de las plataformas, incluyendo tiempos de respuesta prolongados, procesos de denuncia poco transparentes y seguimiento limitado.[21]

Adicionalmente, la magnitud del problema queda oculta por la falta de transparencia sistémica de estas plataformas, que controlan de manera estricta el acceso a la información por parte del público, las personas investigadoras, las organizaciones de la sociedad civil y las personas formuladoras de políticas públicas. Dicho esto, algunas de las empresas de redes sociales más importantes han empezado a reconocer su papel, con plataformas como Meta colaborando con iniciativas de la sociedad civil como StopNCII.org[22] y Take It Down[23] para facilitar la eliminación de las NCII. También han introducido políticas más estrictas prohibiendo tanto las NCII tradicionales como aquellas facilitadas por IA.[24]

En respuesta a estos desafíos, en los últimos años se ha producido un cambio: se ha pasado de culpar a las personas que comparten NCII a exigir que las plataformas rindan cuentas directamente. Las demandas legales recientes ofrecen las primeras pruebas de este cambio. Entre los casos más destacados se incluyen la acción legal de Francia contra Telegram por complicidad en actividades ilegales incluyendo CSAM,[25] la demanda por parte del estado de San Francisco (EE.UU.) en contra de los sitios que crean NCII a través de ultrafalsos facilitados por IA,[26] la demanda en contra de X por el gobierno de Baltimore (EE.UU.),[27] las medidas de Países Bajos contra la facilitación y difusión masiva de NCII facilitadas por IA por parte de Grok,[28] y la demanda contra Meta por el gobierno de Nuevo México (EE.UU.) por permitir daños, incluida la explotación sexual infantil, contra sus usuarios y usuarias.[29]

La UE acuerda prohibir las aplicaciones de "desnudez" para proteger a la ciudadanía

La Unión Europea alcanzó recientemente un acuerdo político para simplificar la implementación del Reglamento de IA (la regulación integral de la UE en materia de inteligencia artificial), al tiempo que refuerza la protección frente a contenidos sexuales nocivos generados por IA. El acuerdo prohíbe los sistemas de IA que crean NCII (incluidas las aplicaciones de "desnudez"), así como CSAM generado por IA. Las instituciones europeas presentaron estos cambios como un intento de equilibrar la innovación, la competitividad y la protección de los derechos fundamentales.[30]

PANORAMA GENERAL DE LOS MARCOS REGULATORIOS Y POLÍTICAS PÚBLICAS EN EL MUNDO

Las NCII facilitadas por IA se basan en un tipo de daño que se ha abordado en marcos políticos y legales por más de una década. Sin embargo, su definición inicial como "pornovenganza" redujo el alcance del problema, ocultando sus dimensiones estructurales y de género, y dejando lagunas en torno al contenido sintético y a la responsabilidad de las plataformas.

A continuación, se presenta un análisis de las tendencias globales de marcos regulatorios en materia de NCII y CSAM, junto con una visión general del marco legal actual en los EE. UU., destacando el rol central de este país como la principal jurisdicción para la gobernanza de la mayoría de las plataformas.

Principales tendencias en la regulación de las imágenes íntimas no consentidas facilitadas por IA

Solo 58 de 190 países han promulgado leyes para proteger a las mujeres contra el ciberacoso, lo que protege a menos de la mitad de la población global, y solo 7 economías ofrecen indemnizaciones y/o compensaciones económicas para las personas sobrevivientes, además de las sanciones penales.[31] En términos de NCII digitales, en 2025, 117 países reportaron iniciativas para abordarlas.[32] La siguiente tabla presenta una selección de legislaciones alrededor del mundo para abordar el problema de las NCII facilitadas por IA:

Legislaciones alrededor del mundo para abordar el problema de las NCII facilitadas por IA

País	Instrumento jurídico	Año	Alcance de la tipificación del delito	Sanciones	Característica destacadas
Australia	Ley de Enmienda al Código Penal (Material Sexual Deepfakes)[33]	2024	Creación y distribución de NCII (incluye aquellas generadas con IA).	Hasta 7 años de prisión.	• Énfasis en la claridad jurídica y la armonización. • El Consejo jurídico advirtió sobre posibles excesos regulatorios; el Senado respaldó el proyecto de ley con recomendaciones de revisión y armonización. • Primer enjuiciamiento bajo el nuevo delito federal en 2026.[34]
Canadá	Ley para la Protección de las Víctimas (Bill C-16, ley para la protección de las víctimas y el resguardo de los menores frente a depredadores)[35]	2026	Para incluir expresamente los ultrafalsos no consentidos, la Ley para la Protección de las Víctimas (*Protecting Victims Act*) prohíbe la distribución de NCII y tipifica como delito la amenaza de distribuir este tipo de contenido, incluidos los ultrafalsos. El Código Penal ya prohibía la distribución de imágenes íntimas sin el consentimiento de la persona representada, pero no contemplaba las amenazas de difundirlas, una práctica frecuente en los casos de sextorsión. Creación de nuevos tipos penales para abarcar ultrafalsos utilizados para CSAM, así como representaciones de bestialismo.	Hasta 10 años de prisión.	• Incremento de la pena máxima por amenazar con distribuir NCII de cinco a diez años cuando el delito se persigue por acusación formal (*indictment*), incluidos los ultrafalsos sexuales. • Incorporación de circunstancia agravante al delito de extorsión cuando este se comete en el contexto de casos de sextorsión. • Restablece todas las penas mínimas obligatorias (*mandatory minimum penalties, MMPs*) que habían quedado sin efecto tras ser declaradas inconstitucionales por la Corte Suprema de Canadá, excepto cuando su aplicación pudiera dar lugar a una pena manifiestamente desproporcionada.

País	Instrumento jurídico	Año	Alcance de la tipificación del delito	Sanciones	Característica destacadas
Dinamarca	Ley Danesa de Derechos de Autor[36]	2025	Uso no autorizado de la imagen y de la voz, protegidas bajo la ley de derechos de autor.	Multas para las plataformas; obligación de eliminar el contenido.	• Protección en dos niveles: salvaguardias generales contra la reproducción digital realista y derechos específicos para artistas. • Regula el contenido de imágenes y audio, y se está utilizando para temas relacionados con los ultrafalsos sexuales. • Aplicación a través de la Ley de Servicios Digitales de la Unión Europea. • Entrada en vigor a partir de julio de 2026.
Corea del Sur	Ley de casos especiales en materia de sanción de los delitos sexuales[37]	2024	Creación, distribución, posesión y consumo de NCII (incluye aquellas generadas con IA).	Hasta 7 años (por producción o distribución); hasta 3 años o multas (por posesión o visualización).	• Desencadenada por la proliferación de contenido de ultrafalsos sexualizados en un chat de Telegram con más de 22,000 integrantes.[38] • Prohibición amplia, incluyendo el consumo.
Reino Unido	Ley de Datos (Uso y Acceso) (DUAA por sus siglas en inglés)[39]	2025	Creación y solicitud de NCII (incluye aquellas generadas con IA).	Hasta 6 meses + multas ilimitadas.	• Se basa en medidas anteriores (Ley de "pornovenganza" del 2015, Ley de Seguridad Online del 2023). • Impulsada por esfuerzos de incidencia.

A pesar de los recientes avances normativos de algunos países, como Canadá, la arquitectura regulatoria en su conjunto suele seguir siendo estructuralmente incompleta. Se identifican seis brechas estructurales interjurisdiccionales en los marcos normativos en torno a la violencia de género facilitada por la tecnología (TFGBV por sus siglas en inglés): 1) definiciones fragmentadas e inconsistentes; 2) predominio de compromisos no vinculantes frente a obligaciones vinculantes; 3) avance desigual a nivel regional; 4) retraso entre la adopción y la implementación; 5) rendición de cuentas limitada por parte de las plataformas y de los sistemas de IA; y 6) brechas persistentes en datos y monitoreo.[40]

Las tendencias antes mencionadas moldean legislaciones de tres maneras: 1) muchos países siguen recurriendo a disposiciones limitadas centradas en delitos específicos en lugar de marcos legales integrales; 2) las leyes sobre cibercrimen y seguridad digital a menudo carecen de una perspectiva de género; 3) la aplicación es débil debido a la limitada capacidad institucional y a la falta de obligaciones vinculantes para las empresas tecnológicas.

Tendencias comunes en la regulación del material de abuso sexual infantil

Si bien el panorama regulatorio sobre el CSAM ha evolucionado significativamente en los últimos años, persisten brechas importantes, especialmente alrededor del contenido generado digitalmente. En un análisis realizado en 2023[41] se evaluó la legislación nacional de 196 países en función de cinco criterios: 1) criminalización del CSAM; 2) definiciones legales; 3) criminalización de delitos facilitados por la tecnología; 4) prohibición de posesión independientemente de la intención de distribuir; y 5) obligación de notificación por parte de los proveedores de servicios de internet. El estudio muestra que únicamente el 32% de los países cuentan con algún tipo de legislación, y que, de estos, el 40% no aborda los delitos facilitados por la tecnología. Únicamente 27 de los 196 cumplen con los cinco criterios, entre ellos Canadá. México cumple con cuatro, fallando en el cumplimiento de la obligación de notificación por parte de los proveedores de servicios de internet.

Esta brecha es aún mayor en el caso del CSAM generado digitalmente. Un estudio de 2024[42] que abarca 49 países reveló que nueve de ellos no tipifican explícitamente como delito este tipo de contenido generado con IA o por medios digitales perjudicial para las personas menores. En cinco de ellos, su tratamiento depende del contexto, y, en otros cuatro (entre ellos México), la legalidad depende de si se representa a un niño o niña real, lo que deja fuera de la ley al contenido sintético en el que no se puede identificar a la persona.

Una encuesta realizada entre personas que han buscado CSAM en la llamada *dark web* reveló que casi tres de cada diez afirmaron haber visto este material de abuso infantil facilitado por IA, mientras que una de cada diez admitió haberlo creado por sí misma con un esfuerzo mínimo.[43]

Estados Unidos: La ley TAKE IT DOWN y más allá

La regulación de las NCII y del CSAM en los Estados Unidos es particularmente relevante para Canadá y México. Esto, dado que sus ecosistemas digitales están profundamente entrelazados con las plataformas basadas en EE.UU. y sus enfoques regulatorios están determinados por los compromisos contraídos en el Capítulo de Servicios Digitales[44] del Tratado entre México, Estados Unidos y Canadá (T-MEC).

Antes del 2025, las personas sobrevivientes en los EE.UU. enfrentaban un marco legal fragmentado entre estados, recursos limitados a nivel federal y la inmunidad de las plataformas por contenidos de terceros bajo la Sección 230 del *Communications Decency Act* (Ley de Decencia en las Comunicaciones).[45] Esto cambió en 2025-2026 con la promulgación de dos leyes históricas de carácter bipartidista. La tabla 2. muestra las nuevas regulaciones en EE.UU. que abordan las NCII facilitadas por IA.

La legislación de EE.UU. sobre las NCII facilitadas por IA

Instrumento	Año de	Enfoque	Disposiciones clave
TAKE IT DOWN Act[46] (Ley de Herramientas para Combatir la Explotación Conocida mediante la Inmovilización de Deepfakes Tecnológicos en Sitios Web y Redes)	2025	Penal	• Tipifica como delito la publicación intencionada de las NCII (incl. aquellas generadas con IA). • Obligación de las plataformas de retirar el contenido en un plazo de 48 horas. • Sanciones económicas y hasta dos años de prisión. • Penas agravadas en los casos que involucren menores de edad.
DEFIANCE Act[47] (Interrumpir la Difusión Explícita de Imágenes Falsificadas y Ediciones No Consensuales)	2026	Civil	• Amplía las opciones de las personas sobrevivientes más allá de la justicia penal. • Permite interponer demandas civiles por daños económicos y emocionales.[48]

Sin embargo, la implementación plantea retos sin resolver. La eliminación efectiva de contenido depende de mecanismos sólidos de verificación de identidad para prevenir fraudes, mientras que el plazo de 48 horas (considerado insuficiente) presiona a las plataformas sin ofrecer financiamiento, ni garantías de cumplimiento. Además, el alcance extraterritorial de ambas leyes depende de la cooperación entre actores globales en un contexto de crecientes tensiones geopolíticas y fragmentación.[49]

En lo que respecta a la protección de menores, el Senado aprobó por unanimidad la Ley *STOP CSAM* en 2025,[50] que amplía la responsabilidad de las plataformas al introducir un criterio de negligencia grave. Esto significa que las plataformas pueden ser consideradas responsables de almacenar o facilitar CSAM, incluso si no tienen conocimiento de eso. La ley aborda tanto la promoción activa como el almacenamiento pasivo de este tipo de material, incluido el facilitado por IA, cerrando un vacío legal que anteriormente permitía a las plataformas eludir responsabilidades alegando desconocimiento. Sin embargo, se advierte que estas nuevas disposiciones podrían ser utilizadas por las empresas para justificar el debilitamiento o abandono del cifrado de extremo a extremo, lo que tendría implicaciones más amplias para la privacidad de las personas usuarias y la seguridad de las comunicaciones.[51]

Junto con estos desarrollos legislativos, el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC, por sus siglas en inglés) ha introducido dos herramientas complementarias: el servicio *Take it Down*,[52] que permite a menores de edad solicitar la eliminación de contenido íntimo sin intervención policial ni procedimientos legales formales; y *CyberTipline*,[53] un sistema centralizado nacional de notificación de la explotación sexual infantil en línea que abarca el grooming, la trata, el CSAM y el contenido facilitado por IA. No obstante, existen algunas limitaciones, entre ellas el hecho de que solo cubren formatos de imagen y video, dejando fuera archivos de audio y/o de texto.[54]

PERFIL DE PAÍS: CANADÁ

Esta sección examina el panorama de las NCII, incluído el CSAM, en Canadá. Se describen los mecanismos regulatorios y de denuncia actuales, y se identifican las principales brechas a la hora de abordar tanto la creación como la distribución de las NCII facilitadas por IA.

Panorama del abuso de las imágenes íntimas no consentidas facilitadas por IA en Canadá

En 2022, la policía registró 896 casos de distribución de NCII.[55] Sin embargo, estimaciones más amplias sugieren que hay aproximadamente 275,000 víctimas y 2.37 millones imágenes por año.[56]

A pesar de esta evidencia, persisten importantes vacíos de datos. La información desagregada (datos desglosados por variables demográficas específicas, como género, sexo, lugar de residencia, origen étnico y otras características relevantes) sobre las NCII facilitadas por IA es en gran medida inexistente, lo que dificulta evaluar cómo está evolucionando el fenómeno en paralelo con la rápida adopción de la IA generativa. Si bien Canadá no ha experimentado un caso detonante de alto perfil, el problema está bien documentado y en crecimiento, con impactos claros en la dignidad, la privacidad, la salud y la participación en la vida pública de las mujeres jóvenes.

La siguiente caja señala casos públicos seleccionados sobre NCII facilitadas por IA en el país.

Casos de NCII facilitadas por IA en Canadá

→ **Un hombre de Quebec es sentenciado por generar pornografía infantil con IA (2023)**[57]

Un hombre fue condenado a ocho años de prisión por utilizar IA para crear videos de CSAM. Se declaró culpable de producir al menos siete videos ultrafalsos y de poseer más de 545,000 archivos de CSAM. Aunque la defensa solicitó una pena menor alegando que no hubo abuso físico, el juez sostuvo que la creación de este tipo de material constituía una nueva vulneración de la integridad sexual de las personas sobrevivientes.

→ **Imágenes facilitadas por IA de niñas desnudas de la escuela de Winnipeg publicadas en línea (2023)**[58]

En 2023, se descubrió que había circulado en línea contenido sexual infantil NCII generadas con IA que involucraba a estudiantes menores de edad de una escuela de Winnipeg. La escuela alertó a las familias, contactó a la policía y activó protocolos de apoyo a personas sobrevivientes, al mismo tiempo colaboraron con *Cybertip.ca* y el Proyecto Arachnid para denunciar y eliminar el contenido.[59] No se presentaron cargos, ya que la policía señaló dificultades probatorias, la reticencia de las personas sobrevivientes de continuar con el proceso, la improbabilidad que se dictara una sentencia y complejidades legales relacionadas con el contenido facilitado por IA.[60]

→ **Desnudos falsos publicados por estudiantes de escuela católica de London (2024)**[61]

Estudiantes de una escuela secundaria local compartieron NCII facilitadas por IA de sus compañeras en chats grupales. La policía abrió una investigación y la escuela advirtió que podría tomar medidas disciplinarias. No obstante, meses después, no se habían presentado cargos contra los estudiantes implicados. El Consejo Escolar católico del distrito de London no reveló si se tomaron medidas disciplinarias y el consejo del sureste de Ontario se negó a responder a preguntas de periodistas.[62]

Marco regulatorio

La *Protecting Victims Act* (Ley para la Protección de las Víctimas) o proyecto de Ley C-16 entró en vigor el 18 de junio de 2026. Esta ley modifica el Código Penal y otras disposiciones legislativas con el objetivo de responder a amenazas actuales y fortalecer la protección de las víctimas. De acuerdo con el Departamento de Justicia de Canadá, *constituye una de las reformas más importantes al Código Penal en generaciones, al buscar reducir la demora en los procesos judiciales, proteger a las víctimas y personas sobrevivientes de violencia de género, incluida la violencia sexual y la ejercida por la pareja, así como reforzar la protección de las infancias rente a depredadores sexuales.*[63]

La ley introduce modificaciones a diversos estatutos penales y del sistema correccional, entre ellas disposiciones relacionadas con la distribución de NCII facilitadas por IA. En particular, amplía el tipo penal de distribución de NCII para incluir representaciones visuales creadas mediante medios mecánicos o electrónicos, como los ultrafalsos. Asimismo, la definición de "imagen íntima" contenida en el Código Penal ahora abarca contenido sintético facilitado por IA, haciendo más sencilla su aplicación. La reforma también restablece penas mínimas obligatorias para diversos delitos, entre ellos la distribución de NCII y el voyeurismo, e incorpora nuevos tipos penales, como la amenaza de distribuir CSAM y la amenaza de difundir NCII, incluidos los ultrafalsos sexuales.[64]

En los próximos meses será importante evaluar la efectividad de estas nuevas medidas, así como los recursos destinados a su implementación, incluyendo la capacitación de operadores del sistema de justicia, cuerpos policiales y personal encargado de brindar apoyo a las víctimas.

Esta nueva ley se centra en los responsables individuales, a diferencia del Proyecto de Ley C-63 (*Online Harms Act*), cuyo enfoque estaba dirigido a imponer obligaciones regulatorias a las plataformas digitales. El Proyecto de Ley C-63 decayó en 2025 tras la disolución del Parlamento con motivo de las últimas elecciones federales. El Proyecto de Ley C-34, presentado en junio de 2026, retoma este enfoque regulatorio con el objetivo de abordar de manera más efectiva los daños en el entorno digital.[65]

A la espera de nuevas obligaciones regulatorias para las plataformas

El 10 de junio de 2026, el gobierno de Canadá presentó el Proyecto de Ley C-34 (*Safe Social Media Act*), que busca ampliar las obligaciones de las plataformas digitales para hacer frente a contenidos nocivos, incluidos los *deepfakes*.

El Safe Social Media Act promulgaría dos nuevas leyes: el Digital Safety Act y el Digital Safety Commision of Canada Act. Su alcance se extendería más allá de las redes sociales para abarcar servicios de *chatbots* impulsados por inteligencia artificial, así como otros servicios digitales, sitios web y aplicaciones. Sin embargo, a la fecha de elaboración de este informe, el proyecto aún se encuentra en una etapa inicial del proceso legislativo (primera lectura), por lo que sus disposiciones podrían sufrir modificaciones significativas. Asimismo, persisten diversos aspectos que deberán definirse con mayor claridad a medida que avance el proceso legislativo.[66]

Protección de la privacidad

Adicionalmente, la Oficina del Comisionado de Privacidad ofrece una vía basada en la protección de datos, en lugar del derecho penal. Cuando los datos personales o la imagen de una persona se utilizan sin consentimiento para generar contenido sexual sintético, el Comisionado puede investigar el cumplimiento organizacional, imponiendo obligaciones a las entidades involucradas en la creación y distribución del contenido, y no únicamente a las personas perpetradoras.[67] Este enfoque cobró relevancia después de que el Comisionado iniciara una investigación contra xAI y X por el uso de su herramienta Grok para generar NCII a inicios de 2026.[68]

Marcos por provincia

Los marcos regulatorios provinciales, por su parte, varían significativamente en su capacidad para abordar las NCII facilitadas por IA. La *Loi visant à contrer le partage sans consentement d'images intimes*[69] (o Ley contra la difusión de imágenes íntimas sin consentimiento) de Québec, que entró en vigor en junio de 2025, define explícitamente una imagen íntima como "cualquier imágen alterada o no, que representa o aparenta representar a una persona desnuda [...] o participando en una actividad sexual explícita". Esta formulación amplía la cobertura a contenido alterado digitalmente y potencialmente sintético, comparable a lo que se ha adoptado en marcos similares en otras provincias. Esto incluye la *Intimate Images Protection Act* (Ley de Protección de Imágenes Íntimas) de la Columbia Británica,[70] que permite a las personas sobrevivientes solicitar tanto la eliminación del contenido como una compensación civil, con el respaldo de un servicio de acompañamiento institucional, así como las de New Brunswick (*Intimate Images Unlawful Distribution Act* o Ley contra la Distribución Ilegal de Imágenes Íntimas, SNB 2022)[71] y de la Isla del Príncipe Eduardo (*Intimate Images Protection Act* o Ley de Proyección de Imágenes Íntimas, RSPEI 1988).[72] En cambio, la redacción de los marcos regulatorios de Alberta y Nueva Escocia es demasiado restrictiva para abarcar claramente el contenido alterado o generado con IA, a pesar de que esta última provincia opera Cyberscan,[73] un centro de recursos especializado en abuso mediante imágenes íntimas. Ontario, sin embargo, no cuenta con un marco provincial en vigor.

En lo que respecta a menores de edad, Ontario y Québec exigen que las instituciones de educación superior cuenten con políticas de respuesta en torno a la violencia sexual, mientras que la mayoría de las otras provincias dejan esto a discreción de las instituciones. Aunque estas medidas ofrecen vías para la eliminación del contenido y compensación, en gran medida, no abordan el daño psicológico a largo plazo de las personas sobrevivientes, ni las dimensiones estructurales más amplias.[74]

La estructura federal de Canadá añade una capa adicional de complejidad. El derecho penal es de materia federal, pero la aplicación de ley es predominantemente responsabilidad provincial y no existe una cláusula de supremacía.[75] Los marcos normativos civiles provinciales, que ofrecen distintos niveles de protección de una provincia a otra, coexisten sin problemas con el derecho penal federal, pero este sistema puede resultar complejo. El resultado es un sistema en el que los marcos de protección civiles más sólidos se concentran en unas pocas provincias y donde el acceso a la justicia de las personas sobrevivientes depende, en gran medida, de su ubicación geográfica.

Mecanismos de denuncia y reparación

El panorama de reparación en Canadá ofrece vías significativas, aunque geográficamente desiguales, para las personas sobrevivientes. Los mecanismos más sólidos existen a nivel provincial, mientras que la supervisión federal desempeña un papel complementario, pero limitado.

La *Ordonnance de cessation ou de prévention*[76] (Orden de cese o prevención) de Québec destaca como el mecanismo de respuesta urgente más estructurado del país. Permite presentar solicitudes expeditas y sumarias mediante formularios oficiales, lo que reduce las barreras procesales para sobrevivientes sin representación legal y permite medidas excepcionales cuando la urgencia exige una intervención inmediata. La *Intimate Images Protection Act* (Ley de Protección de Imágenes Íntimas) de la Columbia Británica también ofrece apoyo institucional que guía a las personas sobrevivientes a lo largo del proceso, además de apoyo emocional y canalizaciones a otros servicios.[77]

En los casos que involucran a menores de edad, Cybertip.ca,[78] la línea nacional en Canadá de denuncia para reportar la explotación sexual infantil en línea, operada por el Centro Canadiense para la Protección de la Infancia, provee un canal especializado de denuncia que cubre delitos como el CSAM, grooming en línea, sextorsión y NCII facilitadas por IA (explícitamente). La plataforma también opera el Proyecto Arachnid, una herramienta tecnológica que emite miles de solicitudes mensuales de eliminación de contenido a plataformas que alojan CSAM.

Vacíos regulatorios, implementación y coordinación

La respuesta de Canadá a las NCII facilitadas por IA sigue limitada por un conjunto de factores estructurales que debilitan su efectividad en la práctica:

→ **Marcos regulatorios de privacidad desactualizados**

El régimen de privacidad de Canadá, diseñado en un contexto previo a la IA generativa, resulta cada vez menos adecuado para abordar los desafíos planteados por los contenidos sintéticos. Esta limitación es particularmente crítica para las infancias y adolescentes, cuya exposición al CSAM facilitado por IA queda fuera del ámbito de aplicación de los marcos actuales.[79]

Además, la ley de privacidad vigente carece de mecanismos de aplicación efectivos, incluyendo sanciones penales y económicas. Como resultado, a pesar de que existen propuestas de reformas, el marco actual opera más como una serie de estándares voluntarios que como un régimen regulatorio vinculante.

→ **Fragmentación institucional y limitaciones de capacidad**

La respuesta de Canadá se ve debilitada por la fragmentación de los marcos jurídicos e institucionales. La aplicación penal, las vías de recursos civiles y protecciones de privacidad operan a través de regímenes en gran medida desconectados (derecho penal federal, sistemas civiles provinciales y supervisión de protección de datos) sin un mecanismo general que garantice coherencia. Como resultado, el acceso de las personas sobreviviente a la reparación de daños y sus niveles de protección varían significativamente según la jurisdicción y la vía jurídica.[80]

La capacidad institucional es otra limitante. En Canadá, la decisión de proceder con cargos penales recae en las fiscalías de la Corona y no en la policía, lo que crea un filtro institucional adicional y da lugar a una desconexión entre la investigación y la presentación de cargos. Adicionalmente, los casos suelen depender de la capacidad de explicar tecnologías complejas a tribunales con conocimientos técnicos limitados, mientras que personas funcionarias reciben capacitación limitada en áreas como la informática forense y las formas de abuso específicas en plataformas. Estos retos se suman a las limitaciones de recursos, la poca claridad en los protocolos de documentación y la incertidumbre legal en torno a los requisitos jurídicos para la evidencia digital.[81]

→ **Identificación de personas perpetradoras y casos transfronterizos**

Identificar a las personas perpetradoras se mantiene como una de las principales barreras operativas. Mientras que los casos que involucran tipos tradicionales de NCII pueden ser trazables, la atribución suele ser difícil en los casos facilitados por IA, lo que hace que el enjuiciamiento sea inviable. Este reto es particularmente grave en casos transfronterizos, dónde la aplicación de la ley doméstica tiene un alcance limitado.

→ **Brechas en la prevención y respuestas institucionales**

Las respuestas preventivas y educativas también siguen siendo desiguales. Mientras los planes de estudio de algunas provincias incluyen componentes sobre violencia sexual y daños digitales, su implementación es inconsistente y depende comúnmente de las personas educadoras y la policía local. Además, y desde el 2021, a nivel educación media superior, los marcos preventivos dedicados a la violencia sexual se han diluido, absorbidos frecuentemente por iniciativas más amplias de equidad, diversidad e inclusión.

→ **Inequidades en el acceso a la justicia**

El acceso a la justicia constituye otra barrera. Las personas con mayores recursos económicos, capital social o con mayor conocimiento de los sistemas legales tienen mayor capacidad para buscar reparaciones o navegar los mecanismos disponibles. En contraste, las comunidades de las Primeras Naciones y racializadas se enfrentan a barreras sistémicas adicionales, incluida la desconfianza histórica hacia las fuerzas del orden y los sistemas de justicia, lo que reduce significativamente las tasas de denuncia y el acceso a apoyo.

PERFIL DE PAÍS: MÉXICO

Esta sección examina el panorama de las NCII, incluyendo el CSAM, en México. Se describen los mecanismos regulatorios y de denuncia actuales, y se identifican las principales brechas a la hora de abordar tanto la creación como la distribución de NCII facilitadas por IA.

Panorama del abuso con imágenes íntimas no consentidas facilitadas por IA en México

Las estimaciones más recientes indican que el 84.46% de las personas sobrevivientes son mujeres, y aquellas que tienen entre 21 y 35 años representan casi un tercio de los casos.[82] Además, el 43.2% de las mujeres y niñas que experimentaron ciberacoso reportaron haber sido amenazadas con la publicación de sus datos personales o material íntimo como forma de extorsión. En el 80% de los incidentes estuvieron implicados hombres cisgénero y en el 70% de los casos fueron identificados como los principales agresores.[83]

La exposición al acoso en línea comienza desde una edad temprana. Las mujeres jóvenes de entre 18 y 24 años tienen 27% más probabilidades de experimentar violencia en línea que sus pares hombres.[84] La mayoría de las niñas reportan que su primera experiencia de acoso en línea sucedió entre los 14 y 16 años, y casi la mitad ha recibido amenazas de violencia física o sexual.[85]

La magnitud del daño se amplifica aún más por los altos niveles de consumo, con México posicionándose entre los cinco países con mayor tráfico a nivel global hacia los sitios de NCII más visitados.[86] El impacto es significativamente más grave para menores de edad, ya que México figura entre los países con las tasas más altas de producción y distribución de archivos de CSAM a nivel global. Ciudad Juárez, al norte del país, concentra por sí sola el 60% de los archivos de CSAM a nivel mundial.[87] Además, los casos reportados incrementaron un 86% en la primera mitad del 2025, siendo las niñas el 59% de la población afectada.[88]

Las siguientes cajas destacan los dos casos más famosos de NCII facilitados por IA en el país.

Casos de NCII facilitados por IA en México

→ **El caso IPN (2023)**[89]
Un caso a gran escala de NCII facilitadas por IA surgió en el Instituto Politécnico Nacional (IPN), donde las autoridades descubrieron 166,000 archivos sintéticos, incluido 20,000 videos, en los que, al menos el 40% involucraron a estudiantes mujeres de entre 17 y 25 años. Un estudiante fue inicialmente arrestado por violencia sexual digital, pero parte de la sanción fue anulada por falta de pruebas. Tras la confirmación que algunos de los contenidos involucraron a menores de edad, se presentaron cargos por posesión y distribución de CSAM, lo que resultó en una sentencia de cinco años de prisión y una multa. El caso sigue parcialmente sin resolverse, con apelaciones en curso y las sobrevivientes denunciando negligencia institucional y revictimización.

→ **Caso Zacatecas (2025)**[90]
Al menos 400 estudiantes mujeres de secundaria y bachillerato del estado de Zacatecas denunciaron la creación y circulación de NCII facilitadas por IA. Las investigaciones sugieren que tres hombres adolescentes de la misma institución crearon y difundieron el contenido, al momento de redactar este informe, todavía no se ha dictado ninguna sentencia.

Marco regulatorio

México cuenta con unos de los marcos legales más amplios del mundo para abordar la violencia digital. Un pilar central es la Ley Olimpia,[91] una serie de reformas legislativas que iniciaron en el 2018 en las que se establece la violencia digital como una categoría jurídicamente reconocida y que criminalizan las violaciones a la intimidad sexual a través de medios digitales, incluyendo la distribución de NCII. Aunque estas reformas van más allá de las

imágenes auténticas para incluir contenido alterado, permitiendo que las NCII facilitadas por IA entren en las definiciones existentes, su aplicación al contenido sintético continúa siendo desigual en la práctica.

Adoptada inicialmente en el estado de Puebla en el 2018, la Ley Olimpia ha sido desde entonces implementada en los 32 estados mexicanos a través de reformas a los códigos penales estatales, criminalizando las NCII a nivel nacional. Sin embargo, esta expansión se ha basado en definiciones jurídicas y terminologías diferentes, lo que ha generado inconsistencias en la manera en que los delitos son definidos, investigados y perseguidos penalmente.[92]

El marco federal se fortaleció aún más en 2021mediante reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia[93] y al Código Penal Federal.[94] Estas reformas incorporaron formalmente la violencia digital al marco jurídico nacional y ampliaron las herramientas de prevención y reparación, aunque no cubren explícitamente las NCII facilitadas por IA.

En los casos vinculados con explotación, 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] establece restricciones sobre la pornografía no consentida, particularmente cuando involucra explotación sexual, menores de edad o personas con discapacidad, o cuando terceros obtienen beneficios del contenido. Estas disposiciones pueden aplicarse en ciertos casos de NCII que, por lo general, suelen conllevar sanciones más severas y se benefician de mecanismos institucionales más sólidos que las disposiciones estándares en materia de violencia digital.[96]

Finalmente, pese a los recientes avances regulatorios, la protección de niñas, niños y adolescentes frente a la violencia digital sigue siendo limitada. El Código Penal Federal[97] define la pornografía infantil como cualquier acto que invlolucre el tráfico, distribución o exhibición de menores mediante escritos, grabaciones, fotografías o imágenes, ya sean reales o simuladas realizadas por una persona que utilice cualquier medio o método. Asimismo, cualquier persona que almacene, compre o rente dicho material incluso sin intención de venderlo o distribuirlo puede ser castigada con hasta cinco años de prisión, además de multas.[98]

Mecanismos de denuncia y reparación

A nivel judicial, la Suprema Corte de Justicia de la Nación ha desarrollado un protocolo para juzgar con perspectiva de género.[99] Este orienta la manera en que los tribunales examinan el contexto, valoran hechos y pruebas, identifican formas interseccionales de discriminación, reconocen estereotipos de género y sesgos, y determinan reparaciones.[100] En materia civil, el Artículo 1916 del Cógido Civil Federal[101] permite reclamar daño moral, un recurso disponible para personas sobrevivientes de difusión de NCII que buscan una alternativa al proceso penal.

A nivel institucional, la Ciudad de México es la única jurisdicción con una agencia especializada en delitos sexuales digitales,[102] pero enfrenta una serie de desafíos. No solo depende de soporte externo para investigaciones técnicas, sino que su personal está principalmente capacitado en trata de personas, lo que refleja una falta de conocimientos especializados en materia digital. La Línea Mujeres[103] ofrece un servicio telefónico que brinda orientación y apoyo a mujeres que experimentan violencia, pero cuando los casos involucran violencia digital son transferidos a la Policía Cibernética de la Guardia Nacional, que no está especializada en materia de género. La protección de menores, por su parte, es coordinada por el Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes,[104] pero no fue diseñado específicamente para abordar las NCII facilitadas por IA.

Muchos de los vacíos que dejan los mecanismos institucionales son cubiertos por la sociedad civil. Organizaciones como Cultivando Género,[105] Defensoras Digitales,[106] Hijas de Internet,[107] Luchadoras,[108] y SocialTic,[109] entre otras, brindan educación sobre seguridad digital, recursos de prevención y apoyo directo a personas sobrevivientes en contextos donde las instituciones formales están ausentes, resultan insuficientes o son inaccesibles.

Actualización normativa de octubre de 2026: nuevas obligaciones para las plataformas digitales

México adoptó un decreto que establece nuevas obligaciones para las plataformas digitales en materia de protección de menores frente a contenidos nocivos, incluyendo medidas de verificación de edad y retiro de contenidos.

Aunque es obligatorio, el decreto no desarrolla criterios técnicos suficientemente detallados para su implementación y supervisión, ni establece sanciones específicas por incumplimiento. El gobierno lo ha caracterizado como no punitivo y ha señalado que podría impulsar una ley con sanciones si las plataformas no cumplen.

Si bien no aborda expresamente las NCII, algunas de sus disposiciones podrían resultar aplicables cuando involucran a menores. Este decreto ilustra los desafíos persistentes para traducir las obligaciones normativas en mecanismos efectivos de rendición de cuentas de las plataformas.

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

Vacíos regulatorios, de implementación y coordinación

A pesar de los mecanismos descritos anteriormente, la respuesta de México frente a las NCII facilitadas por IA sigue siendo restringida por una serie de limitaciones estructurales que evidencian una profunda desconexión entre la amplitud del marco jurídico y la capacidad institucional para operacionalizarlo.

→ **Implementación por encima de legislación**

El problema central en México no es la ausencia de normas, sino la limitada capacidad institucional para implementarlas. El personal del Ministerio Público frecuentemente carece de claridad sobre qué evidencia solicitar, cómo incorporar estos delitos en una investigación o cómo construir casos que resistan el escrutinio judicial. Muchas fiscalías evitan por completo casos de NCII, por temor a que jueces exijan estándares probatorios equivalentes a los requeridos en los casos de tráfico de personas. Estos estándares no solo resultan desproporcionados con respecto a las sanciones involucradas, sino que también son poco adecuados para las NCII facilitadas por IA, donde puede que no existan pruebas tradicionales de evidencia.

Una complicación adicional radica en la propia terminología. El delito está definido bajo distintos nombres, lo que provoca que el personal fiscal interprete y clasifique las conductas basado en sus propios criterios. Esta variabilidad en la interpretación da lugar a inconsistencias desde el primer punto de contacto institucional e incluso puede determinar si un caso avanza o no. En 2021, de las 1,500 denuncias presentadas por distribución de NCII, sólo ocho llegaron a manos de una persona juzgadora para iniciar el procedimiento penal de manera formal ante tribunal, representando el 0.5% de los casos.[110] En cambio, muchos terminan en acuerdos reparatorios o juicio sumario, aunque se desconoce el número exacto.

→ **Capacidad institucional y brechas judiciales**

Las autoridades públicas suelen carecer de capacitación técnica y con perspectiva de género, lo que limita su capacidad para responder eficazmente al abuso digital. Esto se refleja tanto en la escasez de personal especializado, así como en la ausencia de protocolos claros y estandarizados.[111] En la práctica, estas brechas pueden desalentar las denuncias, particularmente cuando las personas sobrevivientes anticipan revictimización, una situación agravada por la persistente minimización del daño digital como "no real" cuando el contenido es sintético.

→ **Carga de la prueba sobre las personas sobrevivientes**

Con frecuencia, se les exige a las personas sobrevivientes que demuestren su credibilidad, recopilen y preserven sus propia evidencia, naveguen procesos probatorios complejos, gestionen las capturas de pantalla, preserven URLs, y manejen procesos con las plataformas e inconsistencias entre las jurisdicciones.[112] A diferencia de los casos que implican daños físicos, el daño psicológico, económico, social y profesional causado por las NCII es difícil de cuantificar mediante herramientas probatorias habituales.

→ **La brecha de protección para menores de edad**

La Ley General de Educación[113] mexicana exige que las escuelas cuenten con protocolos de prevención y respuesta ante la violencia, pero estos no han sido adaptados para abordar el abuso basado en imágenes, violencia digital o contenido facilitado por IA. Las escuelas han desarrollado campañas contra el *bullying* o acoso escolar tradicional, pero tampoco las han trasladado al entorno digital.

→ **Brecha de datos y evidencia**

El panorama de datos en México es insuficiente para diseñar políticas públicas basadas en evidencia en torno a las NCII y el CSAM. Los datos de ciberseguridad del Instituto Nacional de Estadística y Geografía (INEGI) carecen del nivel de detalle necesario para combatir las NCII facilitadas por IA. No existen métricas confiables que distingan el contenido sintético del contenido auténtico, ni un seguimiento integral de los casos desde la denuncia hasta su resolución, ni datos públicos exhaustivos sobre el perfil de las personas perpetradoras (por ejemplo, edad, género y relación con las personas sobrevivientes).

HALLAZGOS COMPARATIVOS CLAVE

Las respuestas de Canadá y México frente a las NCII facilitadas por IA revelan una paradoja presente en ambos países. A pesar de operar desde tradiciones jurídicas, arquitecturas institucionales y contextos de recursos muy distintos, ambos llegan a resultados similares para las personas sobrevivientes, como se muestra a continuación en la tabla siguiente.

Hallazgos comparativos en las respuestas de Canadá y México ante las NCII facilitadas por IA

	México	**Canadá**	**Puntos en común**
Cobertura legal del contenido sintético	La Ley Olimpia, en principio, cubre el contenido modificado/alterado; aplicación inconsistente en las 32 jurisdicciones.	El *Protecting Victims Act* (proyecto de Ley C-16, aprobado) amplía la definición de NCII contemplada en el Código Penal para incluir contenido sintético facilitado por IA, incluidos los ultrafalsos sexuales. Asimismo, tipifica como delito la amenaza de distribuir imágenes íntimas, incluidos los ultrafalsos sexuales.	• Ambos países han avanzado hacia el reconocimiento de los daños facilitados por la IA dentro de los marcos existentes sobre NCII. Sin embargo, la regulación continúa centrándose principalmente en las conductas individuales y sus consecuencias, en lugar de abordar de manera integral el ecosistema de generación y difusión de contenidos a través de IA.
Responsabilidad de las plataformas y prevención	Obligaciones limitadas específicas para las plataformas y un enfoque que depende principalmente de mecanismos de reparación por la vía penal y civil.	La responsabilidad individual se ha fortalecido mediante el *Protecting Victims Act* (Proyecto de Ley C-16, aprobado), mientras que las obligaciones más amplias para las plataformas continúan en desarrollo a través del Proyecto de Ley C-34 (Social Media Act), actualmente en proceso legislativo.	• Actualmente, ninguno de los dos países cuenta con un marco integral que aborde el papel de las plataformas en la prevención, detección y respuesta a la distribución de NCII facilitadas por IA a gran escala.
Capacidad institucional	Prácticamente inexistente fuera de la agencia de la Ciudad de México dedicada a los crímenes sexuales digitales; no hay infraestructura especializada en la mayoría del país.	Fragmentada entre las autoridades federales/provinciales; las fiscalías de la Corona tienen capacidad y alfabetización tecnológica judicial desigual.	• Ambos enfrentan un sistema de justicia poco preparado para manejar la complejidad técnica de los casos de NCII facilitadas por IA.
Mecanismos de reparación	El Artículo 1916 del Código Civil Federal ofrece una alternativa para una indemnización por daños morales. La sociedad civil cubre las brechas críticas que han dejado las instituciones formales.	Los mecanismos de denuncia y reparación se concentran principalmente a nivel provincial. Québec y Columbia Británica cuentan con vías específicas para solicitar el cese o eliminación de imágenes íntimas. Para menores, Cybertip.ca ofrece un canal nacional especializado de denuncia y eliminación de contenido.	• La reparación centrada en las personas sobrevivientes depende de la geografía y de la viabilidad de recursos, no de un marco nacional integral.

	México	Canadá	Puntos en común
Protección de menores	Marcos más sólidos bajo la ley de trata de personas; los perpetradores de menores rara vez son procesados; las escuelas no están preparadas.	Las provisiones de CSAM cubren el contenido facilitado por IA; sistema juvenil flexible; respuestas educativas inconsistentes.	• Ambos tienen marcos legales más sólidos para el CSAM que para las NCII de adultos, sin embargo, las escuelas en ambos países no han adaptado los protocolos de violencia a los ambientes digitales.
Datos y evidencia	No hay suficientes datos desglosados sobre el contenido sintético.	Existen datos agregados sobre las NCII; en su mayoría, las métricas específicas de IA no están disponibles; no hay una categorización de información estandarizada.	• Ninguno de los países puede medir el alcance de las NCII facilitadas por IA; las personas formuladoras de políticas públicas están diseñando respuestas a un problema sin suficiente información.
Acceso a la justicia para personas sobrevivientes	La carga recae sobre las personas sobrevivientes; la revictimización es común; únicamente el 0.5% de las denuncias llegan a los tribunales.	El apoyo jurídico es costoso; la carga de prueba recae sobre las personas sobrevivientes; la vergüenza de las personas sobrevivientes las disuade de denunciar; los grupos vulnerables se enfrentan a barreras agravantes.	• En ambos países, las personas sobrevivientes experimentan una carga desproporcionada; las personas más marginalizadas (las Primeras Naciones en Canadá, las comunidades indígenas en México y las comunidades racializadas, así como los y las menores) se enfrentan a mayores obstáculos para acceder a la justicia.

→ La falta de rendición de cuentas de las plataformas: un problema en ambos países

Among the convergences identified in this Entre las convergencias identificadas en este análisis comparativo, ninguna es más evidente que la limitada capacidad de ambos países para exigir rendición de cuentas a las plataformas digitales. Teniendo en cuenta que la mayoría de las plataformas donde se crean, se distribuyen y se monetizan las NCII facilitadas por IA están basadas en los EE. UU., Canadá y México se enfrentan a una limitación estructural similar para regularlas.

Este desafío es reforzado por el capítulo de servicios digitales del T-MEC, que restringe la capacidad de los gobiernos para imponer requisitos (como lo son la transparencia algorítmica, localización de datos o la representación local) a las plataformas, lo que debilita la soberanía digital y el acceso a la justicia. En la práctica, las plataformas suelen negarse con frecuencia a proporcionar la información necesaria para identificar a las personas perpetradoras, alegando obligaciones en cuestión de privacidad. Aunque cuando el contenido ha sido eliminado, a menudo reaparece, ya que las plataformas se enfrentan a pocas consecuencias o incentivos para promover su detección y la aplicación de la ley.

Estos desafíos se ven además agravados por la naturaleza transfronteriza del daño. Cuando las personas perpetradoras operan a través de las fronteras, las vías de recurso legal se vuelven considerablemente más complejas. Aunque pueden presentarse denuncias, la extradición rara vez es viable, ya que los delitos relacionados con las NCII suelen clasificarse como delitos menores en los marcos de cooperación internacional. Como resultado, muchos casos quedan, en la práctica, fuera del alcance de las autoridades encargadas de su aplicación, independientemente de la solidez de la legislación nacional.

RECOMENDACIONES DE POLÍTICA PÚBLICA

Tanto Canadá como México enfrentan limitaciones estructurales que ningún marco nacional puede resolver de manera aislada: plataformas basadas en Estados Unidos que operan fuera de su alcance regulatorio, inconsistencias conceptuales que dificultan la cooperación transfronteriza y una brecha de protección para personas menores de edad que requiere respuestas educativas coordinadas. Las siguientes recomendaciones abordan estos desafíos compartidos mediante mecanismos multilaterales y bilaterales.

Recomendaciones de política pública transversales

Homologar las definiciones de imágenes íntimas no consentidas facilitadas por IA

→ Aprovechar los mecanismos multilaterales para promover: 1) una definición internacional de la violencia de género facilitada por la tecnología y de la violencia digital de género que incluya las NCII facilitadas por IA; y 2) la cooperación transfronteriza para las respuestas legales en torno a las NCII, incluyendo espacios como la Organización de los Estados Americanos (OEA), en particular la Comisión Interamericana de Mujeres (CIM), el proceso Beijing+30 de ONU Mujeres y los marcos de gobernanza de IA de la OCDE, entre otros.

Aprovechar el Tratado entre México, Estados Unidos y Canadá para la rendición de cuentas de plataformas.

→ Impulsar una posición conjunta sobre la rendición de cuentas de las plataformas en la próxima revisión del T-MEC, tomando como base las fallas documentadas del actual capítulo de servicios digitales.

→ Explorar modelos vinculantes ya existentes, incluyendo las obligaciones de evaluación de riesgos de la Ley de Servicios Digitales de la Unión Europea y el requisito de eliminación en un plazo de 48 horas de la Ley *TAKE IT DOWN* como ejemplos de cómo podrían verse en la práctica estándares vinculantes para plataformas.

→ Promover un acuerdo para establecer estándares mínimos de cooperación de las plataformas en todos los casos de NCII, incluyendo plazos obligatorios de respuesta a solicitudes de información por parte de las autoridades y obligaciones para prevenir la recirculación del contenido reportado.

→ Exigir a las plataformas implementar mecanismos proactivos de detección de CSAM mediante tecnologías existentes de coincidencia de huellas digitales (*hash-matching*) como obligación mínima para ambas jurisdicciones.

Desarrollar mecanismos de cooperación bilateral para casos transfronterizos de imágenes íntimas no consentidas facilitadas por IA

→ Establecer los mecanismos estructurales para el intercambio de conocimiento internacional entre organizaciones de la sociedad civil, profesionales del derecho y actores institucionales; incluidas las visitas de estudio, programas de capacitación conjunta y la documentación compartida de prácticas efectivas.

→ Formalizar dichos intercambios mediante acuerdos bilaterales entre organizaciones, mecanismos de financiamiento conjuntos o un grupo de trabajo permanente Canadá-México sobre las NCII, así como vínculos entre las fiscalías de ambos países y el Centro para la Protección de la Infancia de Canadá.

→ Desarrollar proyectos de investigación bilaterales para seguir documentando los desafíos en torno a las NCII facilitadas por IA, promoviendo investigaciones con enfoques interseccionales y de género.

Abordar las brechas de protección a menores a través de la educación

- → Integrar la alfabetización digital y la seguridad en línea como componentes centrales de los planes de estudio en todos los niveles educativos, incluyendo temas como consentimiento, contenido sintético, manipulación digital, privacidad y dinámicas de ciberacoso, informando al estudiantado sobre sus derechos, mecanismos de denuncia, consecuencias y servicios de apoyo disponibles.
- → Establecer la obligación de adaptar los protocolos escolares de prevención de la violencia para que aborden explícitamente el abuso basado en imágenes, la violencia digital y el contenido facilitado por IA, garantizando que las obligaciones legales ya existentes para las escuelas se extiendan también al entorno digital.
- → Diseñar lineamientos estandarizados y herramientas prácticas para las escuelas. Por ejemplo, un manual orientado a la implementación que traduzca las políticas públicas en protocolos y procedimientos aplicables en el aula.
- → Implementar capacitación continua y con perspectiva de género para personal docente, administrativo y estudiantes. En particular, involucrar a niños y adolescentes hombres en los esfuerzos de prevención para cuestionar normas dañinas y reducir la perpetración de estas conductas.

Recomendaciones específicas para Canadá

El marco jurídico de Canadá cuenta con los elementos fundamentales para abordar las NCII facilitadas por IA; sin embargo, dos brechas estructurales limitan su efectividad: la fragmentación de las capacidades institucionales entre las provincias y las diferencias geográficas en los mecanismos de reparación y protección disponibles para las víctimas. Las siguientes recomendaciones buscan priorizar el cierre de estas brechas.

Fortalecer de los marcos legales

- → Implementar con rapidez las medidas y políticas necesarias para garantizar que *Protecting Victims Act* (Ley para la Protección de las Víctimas) o Proyecto de Ley C-16 sea lo más efectiva posible, particularmente mediante la capacitación de operadores jurídicos, cuerpos policiales y personal encargado de brindar apoyo a las víctimas.
- → Priorizar la aprobación del Proyecto de Ley C-34 y garantizar que cualquier futura legislación federal sobre daños en línea establezca obligaciones vinculantes para las plataformas digitales. Dicha legislación debería ir más allá de medidas voluntarias, como el uso de marcas de agua digitales y filtros algorítmicos para detectar imágenes íntimas sintéticas, e incorporar mecanismos claros de cumplimiento, incluyendo sanciones significativas por incumplimiento.

Fortalecer la capacidad institucional para abordar las imágenes íntimas no consentidas facilitadas por IA

- → Desarrollar programas voluntarios de capacitación interprovincial para fiscales de la Corona, cuerpos policiales y jueces sobre las dimensiones técnicas y probatorias de los casos de NCII facilitadas por IA, incluyendo peritaje forense digital, preservación de evidencia proveniente de plataformas y sentencia con perspectiva de género.
- → Tomar como referencia los marcos existentes en Québec y Columbia Británica como modelos desarrollados entre pares que otras provincias puedan adaptar a sus propios contextos jurídicos e institucionales, facilitando el intercambio horizontal de conocimientos en lugar de una implementación de arriba hacia abajo.
- → Crear un mecanismo de coordinación federal dedicado a articular a las fuerzas de seguridad provinciales, los fiscales de la Corona y las organizaciones de la sociedad civil que trabajan en casos de NCII.

Fortalecer y nacionalizar los mecanismos de reparación centrados en las personas sobrevivientes

- → Extender el modelo de la Orden de cese o prevención de Québec, o un mecanismo equivalente de eliminación urgente de contenido, a todas las provincias, estableciendo un estándar nacional mínimo de reparación de emergencia que no dependa de la ubicación geográfica.
- → Desarrollar una ruta nacional integral de atención para personas sobrevivientes de NCII que integre orientación legal, apoyo para la eliminación de contenido, acompañamiento emocional y referencias a servicios locales, tomando como guía el modelo de acompañamiento de Columbia Británica.
- → Fortalecer el acceso a la asistencia jurídica en casos de NCII que afecten a poblaciones en situación de vulnerabilidad, y explorar mecanismos de financiamiento específicos para organizaciones de la sociedad civil que brindan acompañamiento jurídico de primera línea.
- → Establecer una iniciativa nacional de apoyo a personas sobrevivientes accesible para todas las edades, que ofrezca personal capacitado, orientación legal, apoyo para la eliminación de contenido y acompañamiento emocional vía telefónica y chat. El sistema canadiense *Cybertip.ca* ofrece una base sólida, pero su mandato actualmente se limita a personas menores de 18 años; ampliar su alcance podría contribuir a cerrar esta brecha.

Recomendaciones específicas para México

El desafío de México, más que ser una brecha de legislación, se trata de una brecha en la implementación. El marco de la Ley Olimpia existe en las 32 entidades federativas, pero limitan su efectividad las definiciones inconsistentes, la limitada capacidad institucional especializada y un proceso de denuncia que impone una carga desproporcionada sobre las personas sobrevivientes. Las siguientes recomendaciones priorizan el cierre de estas brechas:

Priorizar la implementación del marco jurídico existente por encima de la creación de una nueva legislación

- → Realizar una auditoría nacional sobre la incorporación de la Ley Olimpia en los códigos penales estatales, con el fin de identificar las definiciones más restrictivas, la aplicación más débil y las tasas de condena más bajas, y utilizar esos hallazgos para orientar intervenciones federales focalizadas.
- → Desarrollar protocolos nacionales vinculantes de implementación para casos de NCII que estandaricen la manera en que las fiscalías clasifican, investigan y construyen los casos bajo las disposiciones existentes. Establecer lineamientos claros para el Ministerio Público que distingan el estándar probatorio requerido para violaciones a la privacidad sexual del que es requerido para delitos de trata de personas.
- → Establecer criterios técnicos, mecanismos de supervisión y sanciones para las plataformas digitales, particularmente para prevenir y abordar las IINC facilitadas por IA.

Fortalecer las capacidades institucionales especializadas a nivel federal y estatal

Expandir el modelo de la agencia especializada operando actualmente en la Ciudad de México, estableciendo requisitos mínimos que incluyan capacidades de policía cibernética in situ, personal especializado y protocolos con perspectiva de género.

Desarrollar un programa nacional obligatorio de capacitación para fiscales, personal investigador y jueces sobre las dimensiones técnicas de los casos de NCII facilitadas por la IA, incluyendo preservación de evidencia digital, cadena de custodia de contenido en línea y herramientas probatorias disponibles para casos en los que los perpetradores operan de manera anónima o de forma transjurisdiccional.

Establecer protocolos formales de cooperación entre fiscalías y organizaciones de la sociedad civil, reconociendo su experiencia técnica y el apoyo que brindan a las personas sobrevivientes como activos institucionales fundamentales.

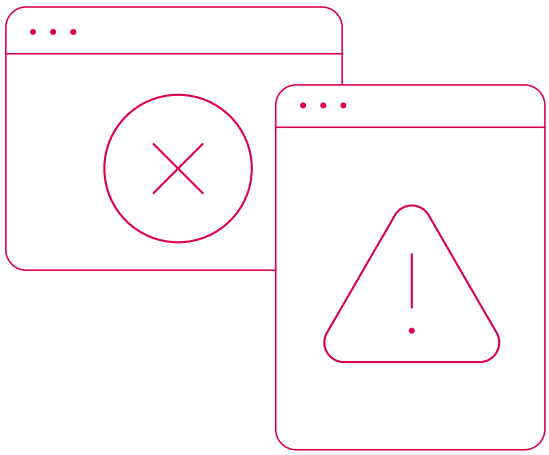
Rediseñar el proceso de denuncia con un enfoque centrado en las personas sobrevivientes

- → Establecer una ruta nacional integral para la denuncia de violencia digital que integre presentación de denuncias, orientación para la preservación de evidencia, asesoría legal, apoyo psicológico y asistencia para la eliminación de contenido en un único mecanismo accesible, eliminando la necesidad actual de que las personas sobrevivientes naveguen jurisdicciones fragmentadas.
- → Eliminar prácticas institucionales que funcionen como barreras para la denuncia, incluyendo exigencias de evidencia fuera del alcance de las personas sobrevivientes o requerimientos de rendir testimonio repetidamente ante múltiples instituciones.
- → Desarrollar un sistema nacional de recolección de datos que dé seguimiento a las denuncias de NCII desde el reporte inicial hasta su resolución, desagregado por tipo de contenido, jurisdicción y resultado, entre otros criterios. Trabajar con organizaciones líderes de la sociedad civil para identificar los tipos de datos que deben recopilarse.

CONCLUSIÓN

Las NCII facilitas por IA ya no constituyen una amenaza emergente, sino una forma arraigada y en expansión de violencia de género facilitada por la tecnología que afecta de manera desproporcionada a mujeres, niñas, niños y adolescentes, con consecuencias que se extienden a todas las dimensiones de sus vidas, incluyendo su seguridad, privacidad, salud mental, oportunidades económicas y capacidad de participar plenamente en la vida pública. En distintas jurisdicciones, la tecnología continúa avanzando más rápido que las políticas públicas, dejando a las personas sobrevivientes frente a sistemas fragmentados que no fueron diseñados para protegerlas.

La comparación entre Canadá y México muestra que, pese a sus contextos distintos, ambos países enfrentan desafíos estructurales similares: capacidad limitada para incidir sobre plataformas basadas en EE.UU., respuestas institucionales fragmentadas y una brecha persistente entre el reconocimiento legal y la implementación efectiva. El desafío central no es la ausencia de legislación, sino la falta de capacidades especializadas, de procesos centrados en las personas sobrevivientes y de gobernanza coordinada necesarios para que las protecciones existentes funcionen en la práctica. La evidencia es clara. Lo que queda por determinar es si ambos países tratarán este problema con la urgencia y seriedad que exige.



Notas

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

2. Conger, K. et al., (2026, Enero 22). 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. (2026, Enero 8). 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. (2025, Octubre 10). 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. (2026, Enero 15). 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. (2024, Junio 3). 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. (2021, April 16). 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 (2026, enero 27). *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. (2025, Julio 14). 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.* Government UK. 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. (2025, Septiembre 15). 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. (2026, Marzo 11). *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. Esta información ha sido compartida por las personas expertas entrevistadas para este informe. Para más información sobre las personas entrevistadas, véase la sección de agradecimientos.

22. Para mayor información: http://stopncii.org

23. Para mayor información: https://takeitdown.ncmec.org/

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

25. Swiss Info (2025, Junio 18). 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. (2025, Junio 2). *City Attorney shuts down 10 websites that create nonconsensual deepfake pornography.* City and County of San Francisco. https://www.sf.gov/news-city-attorney-shuts-down-10-websites-that-create-nonconsensual-deepfake-pornography

27. Robins-Early, N. (2026, Marzo 24). 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. (2026, Marzo 26). 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. (2026, Marzo 24). 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. European Commission. (2026, Mayo 6). The EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens. [Press release]. European Comission. https://ec.europa.eu/commission/presscorner/detail/en/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. (2025, Noviembre 25). 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 of Australia. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2324a/24bd081

34. Schriever, J. (2026, Febrero 26). 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.htm

36. 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. (2025, Septiembre 17). 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. (2024, Agosto 29). 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). *The 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. United States Congress. (2025, Mayo 19). *TAKE IT DOWN Act (S.146, 119th Congress).* https://www.congress.gov/bill/119th-congress/senate-bill/146/text

47. United States Congress. (2025, Mayo 21). *DEFIANCE Act of 2025 (H.R. 3562, 119th Congress).* https://www.congress.gov/bill/119th-congress/house-bill/3562

48. Mithani, J. (2026, Enero 13). 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. United States Congress. (2025, Junio 26). *STOP CSAM Act of 2025 (S.1829, 119th Congress).* https://www.congress.gov/bill/119th-congress/senate-bill/1829/text

51. Bowman, T. (2025, Junio 13). 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. Para mayor información: https://takeitdown.ncmec.org/

53. Para mayor información: 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. (2025, Mazo 12). 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. (2023, Abril 26). Québec 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. (2023, Diciembre 15). 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. Para mayor información: https://cybertip.ca/en/

60. Rosen, K. (2024, Febrero 16). 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. (2024, Abril 4). 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. (2024, Abril 25). 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. Government of Canada (2026, Junio 18). *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

64. Government of Canada (2026, Junio 18). *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

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

67. Office of the Privacy Commissioner of Canada. (2026, January 15). Privacy Commissioner of Canada expands investigation into social media platform X following reports of AI-generated sexualized deepfake images. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260115/

68. Djuric, M. (2026, Enero 15). 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. Québec Government. (2024). *Act to counter non-consensual sharing of intimate images*, CQLR c P-9.0002. https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-9.0002?langCont=en

70. Government of British Columbia. (2026). *Intimate Images Protection Act.* https://www2.gov.bc.ca/gov/content/safety/public-safety/intimate-images/intimate-images-consent

71. Legislative Assembly of New Brunswick. (2022). *Intimate Images Unlawful Distribution Act,* SNB 2022, c 1. https://canlii.ca/t/563w7

72. Prince Edward Island Government. (2021). *Intimate Images Protection Act,* RSPEI 1988, c I-9.1. https://canlii.ca/t/54w8w

73. Para mayor información: https://novascotia.ca/cyberscan/

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. Québec Government. (s.f.). Non-consensual sharing o fan intimate image. https://www.quebec.ca/en/justice-and-civil-status/support-victims-crime/non-consensual-sharing-intimate-image

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. Para mayor información: https://cybertip.ca/en/

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). Deep Fakes: What Can Be Done About Synthetic Audio and Video? *Research and Education. Publication No. 2019-11-E.* https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201911E

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. (2025, Julio 14). 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. (2024, Enero 24). 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. (2025, Julio 16). 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. (2025, Mayo 23). 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. (2025, Noviembre 11). 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. (s.f.). *Ficha técnica Ley Olimpia.* https://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

92. Escobar, C. & Trujano, M. (2023, Abril 25). 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. (2007, Febrero 1). *Ley general de acceso de las mujeres a una vida libre de violencia*. Latest published amendment DOF 15-01-2026 https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

94. Cámara de Diputados del H. Congreso de la Unión. (2021, Junio 1). *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. (2012, Junio 14). *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.* Latest published amendment 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, (s.f.) *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, (s.f.) *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. (1928, Mayo 26, Julio 14, Agosto 31). *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. (s.f.). Violencia digital. https://semujeres.cdmx.gob.mx/violencia-digital

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

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

105. Para mayor información: https://cultivandogeneroac.org/

106. Para mayor información: https://defensorasdigitales.org/

107. Para mayor información: https://hijasdeinternet.org/

108. Para mayor información: https://luchadoras.mx/

109. Para mayor información: https://socialtic.org/

110. Luchadoras. (2022). Acceso a la justicia en casos de violencia digital ¿Qué pasó en 2021?. *Luchadoras MX*. https://luchadoras.mx/defensa-online/justicia-violencia-digital-2021/

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

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

113. Cámara de Diputados del H. Congreso de la Unión. (2019, Septiembre 30). *Ley general de educación.* Latest published amendment DOF 15-01-2026 https://www.diputados.gob.mx/LeyesBiblio/pdf/LGE.pdf

Uso de la IA: se utilizaron herramientas de inteligencia artificial únicamente con fines de ayuda a la redacción, para la revisión lingüística y la reformulación.



IVADO

EON INSTITUTE

con el apoyo de

CANADA FIRST RESEARCH EXCELLENCE FUND

APOGÉE CANADA FONDS D'EXCELLENCE EN RECHERCHE