

## **Riesgos digitales para las infancias: desafíos jurídicos ante la inteligencia artificial generativa**

Digital risks for children: Legal challenges posed by generative Artificial Intelligence

**Marysol Estrella Hernández García**

**Demetrio Hernández Navarrete**

Universidad Autónoma de Guerrero

[20423309@uagro.mx](mailto:20423309@uagro.mx)

### **Resumen**

El artículo analiza los riesgos digitales que enfrentan niñas, niños y adolescentes ante el uso de inteligencia artificial generativa en México. Examina cómo la creación y manipulación de imágenes, voces y videos puede intensificar el acoso, la extorsión, la suplantación de identidad y la exposición de datos personales. A partir del marco de derechos de la niñez y de fuentes jurídicas e institucionales, distingue los riesgos digitales existentes de aquellos amplificados por herramientas generativas. Propone una ruta de protección en tres momentos: prevención desde el diseño, respuesta institucional inmediata y restitución integral de derechos, compatible con la participación de las infancias en entornos digitales.

### **INTRODUCCIÓN**

La vida en internet es algo que afecta a niños y adolescentes en su forma de aprender, de sentir y de relacionarse con otros. Las redes sociales, los videojuegos, los mensajes de texto, las plataformas de la escuela y los sistemas que usan inteligencia artificial permiten que niños y adolescentes ejerzan sus derechos, pero también los ponen en peligro de sufrir acoso, manipulación, robo de identidad, explotación y que se compartan cosas sobre ellos sin que ellos lo sepan ni lo quieran.

La inteligencia artificial generativa cambia la forma en que nos enfrentamos a ciertos riesgos. Esto se debe a que puede crear o cambiar textos, imágenes, sonidos y videos de manera muy realista. Esto hace que sea más fácil para algunas personas crear contenido falso que parece verdadero, adaptar engaños a cada persona y reproducirlos muy rápidamente.

El problema no es que la tecnología en sí sea mala. El problema es cómo las capacidades de la inteligencia artificial generativa interactúan con las decisiones que tomamos como seres



humanos, con la forma en que las empresas funcionan, con la manera en que se tratan los datos y con las respuestas de las instituciones, que a menudo no son suficientes. UNICEF ha advertido que el carácter sintético de una imagen sexualizada no elimina el abuso ni la afectación producida cuando se utiliza la identidad de una persona menor de edad (UNICEF, 2026a; UNICEF, 2026b).

Este artículo analiza los riesgos principales de la inteligencia artificial generativa y los desafíos que presenta para proteger a los niños en México. Lo que aporta este artículo es que diferencia entre la violencia digital que ya existe y la capacidad de la inteligencia artificial para hacer que esta violencia sea mayor. También propone un plan de protección que se divide en tres partes: prevenir problemas desde el principio, responder de inmediato y devolver todos los derechos a los niños. La idea principal es que castigar a los que hacen daño no es suficiente para evitar los daños que pueden ocurrir y propagarse en muy poco tiempo.

## **Desarrollo**

### **I. Infancias y violencia digital en el siglo XXI**

El mundo digital es parte de la vida de los niños y adolescentes. En este mundo, ellos tienen derecho a aprender, a estar informados, a expresarse, a participar, a reunirse con otros y a divertirse. Por lo tanto, la protección legal debe encontrar un equilibrio entre la seguridad y el acceso a la tecnología, en lugar de considerarlas como cosas opuestas. Debe haber condiciones que permitan a los niños y adolescentes participar de manera segura en el mundo digital, sin dejar de respetar su creciente autonomía.

La Convención sobre los Derechos del Niño protege, entre otros, el interés superior de la niñez, la vida privada, el derecho a ser escuchado y la integridad frente a la violencia, el abuso y la explotación sexual (Naciones Unidas, 1989, arts. 3, 12, 16, 19 y 34). La Observación general núm. 25 precisa que esos derechos deben respetarse, protegerse y garantizarse también en el entorno digital, mediante políticas que atiendan la explotación sexual en línea, las agresiones digitales, las vulneraciones de datos y el acceso a mecanismos de reparación (Comité de los Derechos del Niño, 2021).

La violencia digital incluye cosas como amenazas, acoso, publicar fotos sin permiso, crear perfiles falsos, extorsión, contactar con fines de explotación y revelar información privada. Lo que la hace especial no es solo lo que se hace, sino cómo la tecnología permite que se copie, modifique, almacene y compartan cosas. Por ejemplo, una publicación puede ser eliminada de un sitio, pero seguir existiendo en dispositivos, grupos o plataformas, lo que hace que la persona siga perdiendo el control y sufra más.

La forma en que afecta a la gente no es igual para todos. La edad, el género, la discapacidad, la situación económica y familiar, la cultura y el conocimiento sobre tecnología influyen en si se reconoce el peligro y se pide ayuda. Por lo tanto, la seguridad no solo depende de que los niños o sus familias tomen precauciones. El Estado, las escuelas y las empresas que crean, administran o recomiendan contenido también juegan un papel importante en el riesgo y deben hacer cosas para prevenirlo.

## **II. Inteligencia artificial generativa y ampliación de riesgos digitales**

La inteligencia artificial generativa sirve para crear contenido nuevo o cambiar material existente usando instrucciones y patrones que ya han sido procesados. Es importante jurídicamente porque hace que acciones que antes requerían habilidades especiales sean más fáciles. Por ejemplo, se puede alterar una foto, imitar una voz, crear conversaciones falsas o producir muchos mensajes personalizados rápidamente. Esto hace que más personas puedan hacer daño, que el contenido se difunda más rápido y que sea más difícil encontrar de dónde proviene.

Uno de los problemas más serios es cuando se hacen imágenes de niñas, niños y adolescentes de manera sexual. Una foto normal que se encuentra en una red social, en una cuenta de familiares o en un lugar de la escuela, puede usarse para poner la cara de un menor en una situación sexual que no es real. Aunque lo que se muestra en la imagen no haya sucedido, el hecho de usar la identidad de esa persona afecta su privacidad, su dignidad, su reputación y su seguridad.

El contenido también puede utilizarse para hostigar o extorsionar, pues la amenaza de difusión conserva su capacidad de causar miedo, vergüenza, aislamiento o afectaciones escolares. UNICEF sostiene que los materiales sexualizados creados o manipulados mediante inteligencia artificial constituyen una forma de abuso y que incluso los contenidos



completamente sintéticos pueden contribuir a normalizar la explotación sexual infantil y dificultar la identificación de víctimas reales (UNICEF, 2026a; UNICEF, 2026b).

La clonación de voz, la generación de videos y los perfiles falsos permiten simular declaraciones, conversaciones o solicitudes de dinero. También pueden imitar a familiares, docentes o amistades para obtener información privada o crear una apariencia de confianza. Estas capacidades incrementan la eficacia del acercamiento con fines sexuales, ya que un agresor puede adaptar mensajes a la edad, intereses o estado emocional de la víctima y mantener múltiples conversaciones simultáneas.

Hay otro problema que puede ser peligroso: la forma en que se tratan los datos personales. Los menores de edad pueden subir fotos, grabaciones, direcciones o información sobre la escuela sin saber cómo se van a guardar o usar después. Además, familiares, escuelas y otras personas pueden publicar datos que también se pueden utilizar para entrenar sistemas o crear contenido falso. Por lo tanto, la privacidad de los niños no solo depende de lo que decidan ellos mismos, sino también de todas las personas que recopilan, guardan y reutilizan información sobre ellos.

Los sistemas conversacionales añaden riesgos distintos: respuestas falsas presentadas con seguridad, contenidos discriminatorios, recomendaciones inadecuadas para la edad o simulaciones de cercanía emocional. El daño puede intensificarse cuando el sistema desplaza indebidamente la orientación profesional o fomenta una relación de dependencia. UNICEF ha insistido en que el diseño y evaluación de estos sistemas debe considerar las necesidades y etapas de desarrollo de las infancias, no únicamente su eficiencia técnica o comercial (UNICEF, 2025).

La inteligencia artificial generativa no es la causa principal de la violencia digital. Lo que hace es aumentar su alcance, realismo, personalización y velocidad. Esto es importante porque no podemos culpar solo a la herramienta o a la persona que la utiliza. El daño se produce cuando varios factores se combinan, como la conducta del agresor, el diseño del modelo de inteligencia artificial generativa, las decisiones de la plataforma, la disponibilidad de datos y la capacidad de las instituciones para prevenir y contener la difusión de la violencia digital.

### **III. Desafíos jurídicos para la protección de las infancias en México**

El marco jurídico mexicano ofrece fundamentos para proteger a niñas, niños y adolescentes frente a la violencia digital. El artículo 4 constitucional establece que el interés superior de la niñez debe orientar las decisiones y políticas públicas. La Ley General de los Derechos de Niñas, Niños y Adolescentes reconoce el derecho a vivir libre de violencia, protege la intimidad, los datos personales, la honra, la imagen y la reputación, y dispone el acceso y uso seguro de Internet. También obliga a promover medidas frente al ciber acoso y otras formas de violencia realizadas mediante tecnologías de la información (LGDNNA, 2026, arts. 46, 47, 76, 101 Bis 2 y 101 Bis 3).

Estas normas permiten proteger a las personas de la violencia que utiliza inteligencia artificial, aunque la ley no explique cada forma en que se puede hacer. Sin embargo, el hecho de que se reconozcan derechos no soluciona por sí solo problemas como encontrar a los culpables, eliminar contenidos falsos, guardar pruebas o arreglar daños que siguen ocurriendo después de que se publica la primera vez.

En materia de datos personales, la legislación aplicable exige licitud, finalidad, consentimiento, proporcionalidad, información y responsabilidad, y ordena privilegiar el interés superior de la niñez en el tratamiento realizado por sujetos obligados (LFPDPPP, 2025; LGPDPPSO, 2025). La dificultad aparece cuando los datos se mueven entre plataformas, empresas de tecnología y otros procesos automáticos. En estos casos, es difícil saber quién maneja la información, cuánto tiempo la mantiene y cómo se puede pedir que la eliminen. Además, solo porque un adulto dé su permiso, no significa que el uso de los datos sea realmente necesario, esté dentro de los límites adecuados y respete los derechos del menor.

El ámbito penal presenta un problema más específico. El artículo 202 del Código Penal Federal sanciona conductas relacionadas con pornografía de personas menores de dieciocho años e incluye actos sexuales o de exhibicionismo corporal reales o simulados, así como la reproducción, almacenamiento, distribución o transmisión del material (CPF, 2026, art. 202). Sin embargo, su aplicación puede generar dudas cuando se trata de imágenes completamente falsas. En estas imágenes, no se puede identificar a una víctima real y no hay pruebas de que participara en la creación de la imagen. La ley no permite ampliar los delitos penales por



similitud. Por ello, cualquier cambio en la ley debe explicar claramente qué se considera delito en cuanto a la creación, compra, posesión, uso y distribución de este tipo de contenido.

La regulación debe hacer una distinción clara entre situaciones que involucran bienes jurídicos y niveles de daño diferentes. Por ejemplo, utilizar la imagen de un menor de edad identificable, crear material sin base real, conservarlo, distribuirlo o usarlo para extorsionar. Si la fórmula es demasiado amplia, puede violar los principios de taxatividad y culpabilidad. Por otro lado, si la descripción es insuficiente, puede dejar sin respuesta conductas muy dañinas. La incorporación de la expresión “inteligencia artificial” en la ley no reemplaza la necesidad de establecer límites claros.

Otro desafío es determinar quién es responsable. En la creación y difusión del daño pueden participar muchas personas, como quien da las instrucciones, el proveedor del modelo, la plataforma que lo ofrece, la red social que recomienda el contenido y quienes lo almacenan o reenvían. No todos tienen el mismo control ni deben ser responsables de la misma manera. La responsabilidad no debe recaer solo en la persona que causó el daño. Esto es especialmente cierto cuando una empresa conocía los riesgos y obtenía beneficios del servicio. En esos casos, la empresa también debe ser responsable porque no tomó medidas razonables para prevenir o responder al daño. La responsabilidad debe ser compartida de manera justa.

La propagación del daño debe detenerse de inmediato. Para las víctimas, es crucial bloquear la difusión del contenido dañino, recuperar sus cuentas, conservar pruebas y obtener ayuda antes de que concluya el proceso legal.

Las plataformas en línea deben ofrecer canales de comunicación fáciles de usar y procedimientos rápidos para manejar situaciones que involucren a menores de edad. También deben implementar medidas para evitar que se vuelva a subir contenido dañino.

Cuando se elimine el contenido, debe hacerse una revisión humana. También es importante que haya un registro de todo lo que se hace y que las víctimas tengan la oportunidad de apelar, ya que la eliminación automática puede borrar pruebas importantes o afectar contenido legítimo.

La parte internacional de los servicios hace que sea difícil obtener información y tomar medidas. Por eso, es importante que las plataformas, las oficinas de protección, las fiscalías,



las autoridades de datos personales, las escuelas y las autoridades de otros países trabajen juntas. Este trabajo en equipo debe poner a la víctima en el centro, para que no tenga que dar su testimonio muchas veces, para proteger su identidad y para reconocer que la manipulación de su cuerpo, voz o imagen puede hacerle un daño real, incluso si la información no es cierta.

El problema principal no es que no haya normas, sino que están separadas. Los derechos de los niños, la protección de datos, el derecho penal, la responsabilidad de las empresas y los procedimientos para retirar contenido operan por separado. Sin embargo, el daño digital afecta a todos estos ámbitos. Para responder a esto de manera efectiva, es necesario unir todas estas áreas mediante reglas claras, autoridades que trabajen juntas y formas de atención que sean fáciles de entender para las niñas, los niños, los adolescentes y sus familias.

#### **IV. Hacia un modelo preventivo y centrado en derechos humanos**

Para proteger a las infancias de los daños que pueden sufrir en internet, es importante tener un plan de protección que se divida en tres partes: prevención, respuesta rápida y restitución de derechos. Esto no significa que no se deban aplicar sanciones, pero sí que se debe actuar antes de que el daño se produzca.

La primera parte es la prevención. Las empresas que diseñan plataformas y sistemas deben pensar en cómo pueden afectar a los niños y niñas antes de lanzarlos. Deben hacer estudios para ver qué problemas pueden surgir, quiénes pueden ser afectados, y cómo se puede evitar o minimizar el daño. Los resultados de estos estudios deben llevar a medidas concretas, como restricciones técnicas y supervisión continua.

La privacidad y la seguridad deben ser lo más importante. Las empresas deben configurar sus plataformas para que, por defecto, no se compartan datos personales como la ubicación o los contactos. También deben explicar de manera sencilla a los menores cuándo están interactuando con inteligencia artificial y cómo se utilizarán sus datos.

La segunda parte es la respuesta rápida. Las empresas deben hacer que sea fácil para los usuarios denunciar contenido que sea falso o dañino, y deben actuar rápido cuando reciben una denuncia. Las autoridades también deben tener planes claros para recibir denuncias y actuar en consecuencia. La tercera parte es la restitución integral. Cuando se produce un daño,



no basta con eliminar el contenido ofensivo. Es necesario ayudar a la víctima a recuperarse, lo que puede incluir asistencia psicológica, jurídica, y medidas para proteger su identidad.

Para que este modelo funcione, hay cuatro condiciones clave. La primera es la transparencia. Las empresas deben explicar claramente cómo funcionan sus plataformas y cómo manejan los datos. La segunda es la alfabetización digital. Es importante y necesario que los usuarios, sus familias y educadores sepan cómo usar Internet de manera segura. La tercera es la participación es decir los menores deben tener voz en la creación de políticas y mecanismos de denuncia. La cuarta es la supervisión pública para ello necesitamos mecanismos para asegurarnos de que las empresas y las autoridades cumplan con sus obligaciones.

La protección no debe significar prohibir el acceso a la tecnología. Lo importante es encontrar un equilibrio que permita a las infancias usar internet de manera segura y beneficiosa. El objetivo es distribuir las responsabilidades y crear condiciones para un uso seguro. Lo que más importa es el bienestar de los niños, niñas y adolescentes, y esto se logra cuando se toman decisiones concretas y verificables para protegerlos.

## **CONCLUSIONES**

La inteligencia artificial generativa aumenta los riesgos digitales que ya existen porque hace que sea más fácil crear contenido sexualizado, copiar voces, suplantar identidades, personalizar trampas y reutilizar datos personales. El daño que puede causar no solo depende de la herramienta en sí, sino también de cómo la utiliza la persona, las decisiones de diseño, la infraestructura de las plataformas y cómo responden las instituciones.

En México, hay bases constitucionales y legales para proteger a los niños, pero es difícil responder a contenido falso que se propaga rápidamente y cruza diferentes jurisdicciones debido a que los derechos de los niños, la protección de datos, el derecho penal y la responsabilidad empresarial están fragmentados. Es necesario actualizar las normas para definir claramente las conductas y los niveles de intervención, respetar la legalidad penal y establecer obligaciones adecuadas según el control y conocimiento de cada persona o entidad involucrada.

El modelo que se propone busca ordenar la protección en tres etapas: prevención desde el diseño, respuesta inmediata y restitución completa. Esto permite integrar evaluaciones de

impacto, privacidad desde el principio, mecanismos de denuncia y retiro, preservación de pruebas, protocolos institucionales y atención a las víctimas. El objetivo no es mantener a los niños y adolescentes alejados de la vida digital, sino asegurarse de que la innovación sea compatible con su dignidad, seguridad, privacidad, autonomía y desarrollo integral.

## REFERENCIAS

Cámara de Diputados del H. Congreso de la Unión. (2025). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Nueva ley publicada en el Diario Oficial de la Federación el 20 de marzo de 2025. Última reforma publicada el 14 de noviembre de 2025.

Cámara de Diputados del H. Congreso de la Unión. (2025). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Nueva ley publicada en el Diario Oficial de la Federación el 20 de marzo de 2025. Última reforma publicada el 14 de noviembre de 2025.

Cámara de Diputados del H. Congreso de la Unión. (2026). Código Penal Federal. Texto vigente. Última reforma publicada en el Diario Oficial de la Federación el 13 de marzo de 2026.

Cámara de Diputados del H. Congreso de la Unión. (2026). Constitución Política de los Estados Unidos Mexicanos. Texto vigente. Últimas reformas publicadas en el Diario Oficial de la Federación el 2 de junio de 2026.

Cámara de Diputados del H. Congreso de la Unión. (2026). Ley General de los Derechos de Niñas, Niños y Adolescentes. Texto vigente. Última reforma publicada en el Diario Oficial de la Federación el 15 de enero de 2026.

Comité de los Derechos del Niño. (2021). Observación general núm. 25 (2021), relativa a los derechos de los niños en relación con el entorno digital (CRC/C/GC/25). Naciones Unidas.

Naciones Unidas. (1989). Convención sobre los Derechos del Niño. Asamblea General de las Naciones Unidas.

UNICEF. (2025). Guidance on AI and children. Version 3.0. UNICEF Office of Strategy and Evidence-Innocenti.

UNICEF. (2026a). Artificial intelligence and child sexual abuse and exploitation. United Nations Children's Fund.

UNICEF. (2026b). Deepfake abuse is abuse: Statement on AI-generated sexualised images of children. United Nations Children's Fund.