

H. Congreso del Estado de Nuevo León



LXXVII Legislatura

PROMOVENTE: C. MARÍA FERNANDA GARZA ESPINOSA, INTEGRANTE DE LA ASOCIACIÓN CIVIL DENOMINADA "FUNDACIÓN DUQUE PARA EL APOYO DE LA FAMILIA Y LAS ARTES

ASUNTO RELACIONADO: MEDIANTE EL CUAL PRESENTA INICIATIVA DE REFORMA AL ARTÍCULO 271 BIS 5 DEL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN; ADICIÓN DE UN ARTÍCULO 1813 BIS IV AL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN Y POR ADICIÓN DE UN ARTÍCULO 1813 BIS V DEL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN, EN RELACIÓN A LA PROTECCIÓN DE LA DIGNIDAD, LA IDENTIDAD Y LA VIDA PRIVADA DE LAS PERSONAS, FRENTE A NUEVAS FORMAS DE VIOLENCIA DIGITAL

INICIADO EN SESIÓN: Miércoles 25 de Febrero de 2026

SE TURNÓ A LA (S) COMISIÓN (ES): DE LEGISLACIÓN, DE JUSTICIA Y SEGURIDAD PÚBLICA

Mtro. Joel Treviño Chavira
Oficial Mayor

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES AL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN, EL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN Y EL CÓDIGO DE PROCEDIMIENTOS CIVILES DEL ESTADO DE NUEVO LEÓN.

La que suscribe, **María Fernanda Garza Espinosa**, en mi carácter de integrante de la Asociación Civil denominada "Fundación Duque para el Apoyo de la Familia y las Artes", así como ciudadana neoleonés, con fundamento en lo establecido en los artículos 86 y 87 de la Constitución Política del Estado Libre y Soberano de Nuevo León; así como lo dispuesto en los numerales 102, 103 y 104 del Reglamento para el Gobierno Interior del Congreso del Estado de Nuevo León, se somete a consideración de esa Honorable Asamblea, la iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones al Código Penal para el Estado de Nuevo León, el Código Civil para el Estado de Nuevo León y el Código de Procedimientos Civiles del Estado de Nuevo León:

EXPOSICIÓN DE MOTIVOS

La inteligencia artificial¹ se ha consolidado como una de las tecnologías más influyentes del siglo XXI, con impactos relevantes en ámbitos como la salud, educación, industria, seguridad y administración pública. En ese sentido, diversos organismos internacionales han reconocido que ésta posee un alto potencial para el desarrollo social y económico, siempre que su implementación se realice de manera ética, responsable y conforme a derechos humanos².

Así, la IA puede definirse como el conjunto de sistemas informáticos capaces de realizar tareas que normalmente requieren inteligencia humana, tales como el reconocimiento de patrones, el procesamiento del lenguaje natural, la toma de decisiones automatizadas y la generación de contenidos; estos sistemas se apoyan, principalmente, en técnicas de *machine learning* y *deep learning*, las cuales permiten que los algoritmos aprendan con base a grandes volúmenes de datos³.

¹ En lo subsecuente IA.

² OCDE – Principles on Artificial Intelligence (2019). <https://oecd.ai/en/ai-principles>

³ Russell, S., Norvig, P., *Artificial Intelligence: A Modern Approach* (4ª ed., 2021). <https://aima.cs.berkeley.edu/>

No obstante, junto con sus beneficios, la IA también ha generado riesgos jurídicos y sociales relevantes, particularmente cuando se utiliza sin controles adecuados o con fines ilícitos, dado que dichos sistemas pueden ser empleados para amplificar conductas dañinas preexistentes, reproducir sesgos estructurales y facilitar nuevas formas de violencia, acoso o manipulación, especialmente en redes sociales.

En ese contexto, organismos internacionales han recalcado que la regulación de la inteligencia artificial no debe partir de una lógica prohibicionista, sino de un enfoque basado en riesgos y en la protección de derechos fundamentales; la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) ha señalado que los Estados tienen la obligación de prevenir los usos de la IA que puedan causar daño, garantizando al mismo tiempo la innovación tecnológica y la libertad de expresión⁴.

En ese sentido, uno de los principios más relevantes para abordar en la regulación de la IA es el de neutralidad tecnológica, conforme al cual el derecho no regula la tecnología en sí misma, sino los usos y efectos jurídicamente relevantes que se derivan de ella; bajo este principio, la inteligencia artificial no es considerada intrínsecamente lícita o ilícita, sino que lo relevante es el impacto y alcance que su utilización produce sobre los derechos de las personas⁵.

En consecuencia, se entiende que el desafío no consiste en limitar el desarrollo de la inteligencia artificial, sino en establecer límites claros frente a su uso abusivo, especialmente cuando ésta afecta derechos personalísimos como la dignidad humana, la vida privada y la integridad personal, puesto que, cuando una tecnología permite la comisión de daños graves de manera más rápida, masiva o difícil de rastrear, el Estado tiene una obligación reforzada de intervenir normativamente para prevenir y mitigar dichos impactos⁶.

En el orden jurídico mexicano, la protección de la dignidad humana, el libre desarrollo de la personalidad, la vida privada y la propia imagen constituyen ejes rectores del sistema de

⁴ UNESCO- Recommendation on the Ethics of Artificial Intelligence (2021). <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

⁵ Brownsword, R. "Law, regulation, and technology: The bigger picture", *Elgar Online*, (2019). <https://www.elgaronline.com/edcollchap/book/9781803921327/chapter2.pdf>

⁶ Mantelero, A. "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment" (2020). Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3395012

derechos fundamentales⁷. El artículo 1º de la Constitución Política de los Estados Unidos Mexicanos establece la obligación de todas las autoridades de promover, respetar, proteger y garantizar los derechos humanos conforme a los principios de universalidad, interdependencia, indivisibilidad y progresividad, lo que implica adoptar medidas legislativas que prevengan y sancionen las formas contemporáneas de violencia que afectan dichos derechos en entornos digitales y tecnológicos⁸.

Uno de los ámbitos en los que estos riesgos se manifiestan con mayor claridad es la generación automatizada de contenidos, particularmente cuando se emplean sistemas de IA para crear materiales falsos que simulan la identidad de personas reales, generando no sólo problemas de desinformación, sino también afectaciones directas a derechos humanos, al permitir la atribución de conductas inexistentes a una persona sin su consentimiento, con consecuencias reales en su vida personal, profesional y social.

A nivel comparado, distintos marcos regulatorios han comenzado a adoptar un enfoque basado en niveles de riesgo para la regulación de la inteligencia artificial; la Unión Europea, por ejemplo, ha reconocido que ciertos usos de IA, en particular aquellos que afectan la identidad, autonomía o los derechos fundamentales de las personas, requieren controles más estrictos y respuestas normativas específicas, sin que ello implique una prohibición general del desarrollo tecnológico⁹.

Asimismo, organismos técnicos como el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) han desarrollado marcos de gestión de riesgos en materia de inteligencia artificial, destacando la necesidad de que los sistemas de IA sean confiables, transparentes y responsables, especialmente cuando su utilización puede generar impactos adversos en individuos o grupos sociales¹⁰.

Desde esta perspectiva, la regulación de la IA se concibe como un ejercicio de equilibrio normativo; por un lado, se trata de promover la innovación y el desarrollo tecnológico y, por

⁷ Carbonell Sánchez, Miguel, Los derechos fundamentales y su interpretación, México, UNAM, 2020. Disponible en: <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3826/6.pdf>

⁸ Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 5 de febrero de 1917, última reforma publicada en el DOF el 15 de octubre de 2025.

⁹ European Commission, "European approach to artificial intelligence", 2018. Disponible para su consulta en: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

¹⁰ National Institute of Standards and Technology of Commerce, "AI Risk Management Framework 1.0" U.S. Department of Commerce, January, 2023. <https://doi.org/10.6028/NIST.AI.100-1>

otro, prevenir, sancionar y reparar los usos que resulten lesivos para los derechos humanos, como cuando dicha tecnología se utiliza para generar contenidos sintéticos que pueden convertirse en instrumentos de violencia digital, como ocurre con los determinados *deepfakes* no consensuados.

En consecuencia, la presente iniciativa parte del reconocimiento de que la inteligencia artificial no debe ser prohibida, pero sí regulada cuando su utilización se traduce en una vulneración directa de derechos fundamentales, por tanto, resulta necesario que el marco jurídico del Estado de Nuevo León establezca límites claros al uso de tecnologías de IA en aquellos supuestos en los que se empleen para causar daño a las personas, particularmente en contextos de violencia digital y de género.

Ahora bien, el término *deepfake* se utiliza para describir contenidos audiovisuales generados o manipulados mediante técnicas avanzadas de inteligencia artificial, particularmente redes neuronales profundas (*deep learning*), que permiten sustituir, alterar o simular la imagen, la voz o los gestos de una persona con un alto grado de realismo¹¹. Estas tecnologías han evolucionado de forma acelerada los últimos años, reduciendo las barreras técnicas y económicas para su uso, lo que ha ampliado tanto sus aplicaciones legítimas como su potencial de abuso¹².

En suma, los *deepfakes* se producen a partir de algoritmos de aprendizaje profundo que analizan grandes volúmenes de datos visuales y auditivos para identificar patrones faciales, expresiones, movimientos y modulaciones de voz; una vez entrenado, el sistema puede generar contenido artificial que imita con notable precisión la apariencia y comportamiento de una persona real, incluso en situaciones que nunca ocurrieron, lo que dificulta que el público en general pueda distinguir entre contenido auténtico y material manipulado¹³.

A diferencia de otras formas tradicionales de edición audiovisual, **los *deepfakes* no se limitan a modificar imágenes existentes, sino que pueden crear representaciones**

¹¹Chesney, Robert and Citron, Danielle Keats, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security (July 14, 2018). Available at SSRN: <https://ssrn.com/abstract=3213954> or <http://dx.doi.org/10.2139/ssrn.3213954>

¹²Westerlund, M. 2019. "The Emergence of Deepfake Technology: A Review.", *Technology Innovation Management Review*, 9(11): 40-53. <http://doi.org/10.22215/timreview/1282>

¹³Kietzmann, Jan, W. Lee, Linda, et.al., "Deepfakes: Trick or treat?", *Business Horizons*, Volume 63, Issue 2, 2020, Pages 135-146, ISSN 0007-6813, <https://doi.org/10.1016/j.bushor.2019.11.006>

completamente nuevas de una persona, atribuyéndole palabras, acciones o contextos ficticios¹⁴.

Diversas investigaciones académicas han demostrado que el impacto de los *deepfakes* trasciende el ámbito tecnológico, al generar consecuencias reales en la reputación, la vida privada y la integridad emocional de las personas afectadas. En particular, los contenidos de carácter íntimo o sexual, creados sin consentimiento, han sido identificados como una de las formas más extendidas y dañinas de esta práctica, con efectos psicológicos comparables a otra forma de violencia digital¹⁵.

Además, se ha identificado que los *deepfakes* se utilizan de manera desproporcionada contra mujeres, especialmente en contextos de violencia de género digital; investigaciones indican que un alto porcentaje del contenido *deepfake* disponible en internet tiene carácter sexual y se dirige mayoritariamente a mujeres sin su consentimiento, lo que evidencia un patrón de desigualdad y cosificación que refuerza dinámicas estructurales de violencia¹⁶.

De acuerdo con “*Deepttrace*”, en 2019 aumentó al doble la cantidad de *deepfakes* encontrados en Internet; tan es así, que de un total de 14,678 *deepfakes* encontrados en 2019, el 96% son pornográficos, con un total de 134 millones de vistas; nueve sitios web están dedicados exclusivamente a *deepfakes* pornográficos; y ocho de cada diez sitios pornográficos aloja *deepfakes*. Revelando que la totalidad de los sitios web de *deepfakes* pornográficos ataca y daña a las mujeres¹⁷.

Asimismo, en 2023 se documentó uno de los casos más grandes en México de violencia sexual digital con uso de inteligencia artificial, en el cual un exalumno tomó fotografías de alumnas desde redes sociales para alterarlas con IA, sexualizarlas y simular desnudos, de modo que el daño no dependió de que existiera una imagen íntima previa sino de convertir fotos cotidianas en material sexual simulado sin consentimiento. Además, lo que volvió el caso especialmente grave, fue la escala reportada, decenas de miles de videos y más de cien mil imágenes vinculadas, lo cual apuntó a una práctica sistemática y no a un “montaje

¹⁴ Diel, A., Lalgí, T., Mellis, F., et al, op. cit

¹⁵ Henry, N., & Flynn, A. “Image-based sexual abuse: Online distribution channels and illicit communities of support”. *Violence Against Women*, (2019). 25(16), 1932–1955. <https://doi.org/10.1177/1077801219863881>

¹⁶

¹⁷ Bañuelos Capistrán, Jacob. 2020. “Deepfake: La Imagen En Tiempos De La Posverdad”, *Revista Panamericana de Comunicación* 2 (1): 51-61. <https://doi.org/10.21555/rpc.v0i1.2315>

aislado”, por eso mismo el impacto para las víctimas se vuelve doble: por la humillación inmediata y por la imposibilidad de controlar una difusión masiva¹⁸.

De la misma forma, en Zacatecas se reportó un caso donde estudiantes habrían generado con IA un “catálogo sexual” usando rostros e imágenes de compañeras y compañeros, revelando cómo la IA puede fabricar contenido íntimo simulado a partir de material común y, en consecuencia, ampliar el riesgo en entornos escolares, esto, ya que no se requiere “filtrar” una foto real para violentar, sino que basta con editar y circular. En ese sentido, el contexto escolar agrava la afectación porque la difusión ocurre dentro de una comunidad donde la víctima convive a diario con quienes vieron, comentaron o compartieron el montaje, así que el daño no termina en la pantalla sino que se traslada a la vida cotidiana con consecuencias psicoemocionales y posibles dinámicas de amenaza o extorsión¹⁹.

En suma, durante 2025 se difundió ampliamente el caso de la influencer Alana Flores, a partir de la circulación en redes sociales de una supuesta “imagen íntima” atribuida a su persona, la cual resultó ser falsa y presuntamente generada mediante técnicas de manipulación digital tipo deepfake. La afectada anunció la interposición de acciones legales, lo que evidencia que este tipo de agresiones no constituye un fenómeno abstracto o limitado a otros contextos internacionales, sino una problemática real y presente en el ámbito nacional y local. Este caso permite dimensionar cómo la creación y difusión de contenido íntimo sintético puede generar afectaciones inmediatas a la reputación, la vida privada y la integridad de las personas, aun cuando el material sea completamente fabricado.²⁰.

En razón de lo anterior, es evidente que este tipo de conductas forman parte de la violencia estructural y de las desigualdades persistentes en el entorno digital²¹, pues, la evolución de las tecnologías de inteligencia artificial ha evidenciado nuevas formas de agresión que

¹⁸ Consultable en la siguiente liga electrónica:
<https://www.elfinanciero.com.mx/cdmx/2025/05/23/caso-diego-n-dan-5-anos-de-carcel-a-exalumno-de-ipn-acusado-de-violencia-sexual-con-ia/>

¹⁹ Consultable en la siguiente liga electrónica:
<https://vanguardia.com.mx/noticias/mexico/adolescentes-crean-catalogo-sexual-usando-ia-con-fotos-de-400-alumnos-de-secundaria-EA18094752>

²⁰ Consultable en la siguiente liga electrónica:
<https://www.proceso.com.mx/nacional/2025/5/28/la-influencer-alana-flores-denuncia-haber-sido-victim-a-de-deepfakes-tomara-acciones-legales-351990.html>

²¹ Naciones Unidas, “A/HRC/38/47: Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos”, Consejo de Derechos Humanos de las Naciones Unidas, 2018. Disponible en: <https://docs.un.org/es/A/HRC/38/47>

afectan de manera diferenciada a determinados grupos, particularmente a mujeres y jóvenes, quienes suelen ser las principales víctimas de la creación y difusión de contenidos íntimos no consentidos, de manera que, la denominada brecha o desigualdad digital no sólo se manifiesta en el acceso a la tecnología, sino también en la exposición desproporcionada a riesgos y violencias facilitadas por el entorno digital.

En este contexto, el reconocimiento de los deepfakes como una modalidad específica de violencia digital resulta indispensable para dotar a las autoridades de herramientas claras de actuación y garantizar mecanismos efectivos de protección y reparación para las víctimas. Si bien el marco normativo estatal ha incorporado disposiciones orientadas a prevenir y sancionar la violencia digital, la rápida evolución de las tecnologías de inteligencia artificial ha generado supuestos que no siempre encuentran una respuesta expresa en la legislación vigente, particularmente en los ámbitos penal y civil.

Desde esta perspectiva, la presente iniciativa propone armonizar el marco jurídico del Estado de Nuevo León con las disposiciones ya existentes en materia de violencia digital, incorporando en el Código Penal y en el Código Civil referencias específicas a la creación y difusión de contenidos íntimos o sexuales sintéticos generados mediante inteligencia artificial. Lo anterior, reconociendo que los deepfakes constituyen una forma emergente de violencia digital que puede afectar directamente derechos como la dignidad humana, la vida privada, la integridad personal y la igualdad de género, y que su atención requiere herramientas jurídicas claras para su prevención, sanción y reparación.

En esa tesitura, la utilización de IA para la creación de *deepfakes*, no consensuados, constituye una modalidad emergente de violencia digital, caracterizada por la instrumentalización de la identidad, la imagen y el cuerpo de las personas con fines de humillación, control, desacredito o explotación. Así, a diferencia de otras formas de violencia, los *deepfakes* introducen un elemento adicional de gravedad al fabricar representaciones falsas altamente realistas, capaces de producir daños reales y persistentes en la vida de las víctimas²².

La violencia no se limita a la existencia de contacto físico o a la veracidad del contenido difundido, sino que puede materializarse a través de actos simbólicos y psicológicos, entre

²² Diel, A., Lalgí, T., Mellis, F. et al., op.cit, p. 2 y 12

otros, que afectan la dignidad humana y la integridad personal, esto, dado que los *deepfakes* no consensuados son una forma de violencia que opera mediante la apropiación indebida de la identidad y la imposición de narrativas falsas sobre la persona afectada²³.

Diversas investigaciones han documentado que los *deepfakes* de contenido íntimo o sexual generan impactos psicológicos severos en las víctimas, incluyendo ansiedad, depresión, estrés postraumático, aislamiento social y afectaciones a la autoestima, los cuales se ven agravados por la sensación de pérdida de control sobre la propia imagen y por la dificultad para eliminar completamente el contenido una vez que ha sido difundido en plataformas digitales²⁴.

En la práctica, las personas que enfrentan la difusión de un *deepfake* íntimo o sexual se encuentran, con frecuencia, en una situación de desventaja inmediata, pues el daño ocurre en minutos, mientras que las vías institucionales disponibles suelen operar en plazos mucho más largos, por lo que, aún cuando existe disposición para denunciar, el primer obstáculo suele ser probatorio y operativo, como lo es identificar el origen de contenido, documentar su circulación antes de que sea eliminado o replicado, y preservar evidencia digital en un entorno donde las publicaciones se duplican y migran entre plataformas y canales; de esa manera no sólo se dificulta la investigación y la persecución, sino que también agrava la afectación emocional y reputacional, pues la víctima enfrenta la incertidumbre de no saber cuántas copias existen ni dónde volverán a aparecer²⁵.

En ese sentido, la violencia derivada de los *deepfakes* no se agota en el plano emocional, sino que puede extenderse a consecuencias laborales, económicas y sociales, tan es así que, estudios empíricos han señalado que las personas afectadas por este tipo de contenido pueden enfrentar despidos, exclusión profesional, estigmatización comunitaria y deterioro de sus relaciones personales, aun cuando se demuestre que el material es falso²⁶.

²³ Chesney y Citron, op. cit., pp. 1772-1774.

²⁴ Brigham, Natalie Grace, et al., "Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery." *Twentieth Symposium on Usable Privacy and Security (SOUPS)*. Agosto 2024. Disponible en: <https://arxiv.org/pdf/2406.05520>

²⁵ Allah Rakha, Naeem, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations", *Mex. law rev.* 2024, vol.16, n.2 pp.23-54. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-05782024000100023&lng=es&nrm=iso. Epub 09-Mayo-2025. ISSN 2448-5306. <https://doi.org/10.22201/ijj.24485306e.2024.2.18892>

²⁶ Henry, N., y Powell, A. (2016). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse*, 19, (2), 195-208. <https://doi.org/10.1177/1524838016650189>. Disponible en: <https://journals.sagepub.com/doi/10.1177/1524838016650189>

Así, uno de los puntos más críticos es comprender que la remoción o “baja” del contenido (cuando se logra), no equivale a una reparación del daño, sino que tiene efectos que permanecen aún después de eliminar una publicación, ya que pueden existir capturas de pantalla, circulación en grupos cerrados o sitios no cooperantes, y un impacto reputacional que se vuelve difícil de revertir. Además de que la víctima puede enfrentarse a dinámicas de revictimización, presión social para “probar” que es falso (revictimización), así como cuestionamientos sobre su vida privada, o incluso uso del material para extorsión o coerción, por lo que es necesario ir más allá de un enfoque centrado exclusivamente en el contenido y reconocer que el fenómeno involucra derechos personalísimos (imagen, identidad, privacidad, dignidad) y daños que requieren vías efectivas de tutela²⁷.

En el caso particular de los *deepfakes* de naturaleza sexual, existe evidencia consistente de que estos contenidos se insertan en patrones de violencia digital que afectan de manera desproporcionada a mujeres y niñas, reforzando prácticas de cosificación y control en el entorno digital, tan es así que organismos internacionales han advertido que la inteligencia artificial está amplificando formas de abuso como el acoso, la extorsión y la manipulación de imágenes, con consecuencias tangibles en la vida real²⁸.

La afectación trasciende la esfera individual, pues impacta el entorno social de la persona y restringe su participación pública, su acceso al empleo, su seguridad personal y el ejercicio de sus derechos en los ámbitos político, comunitario y laboral²⁹.

Por ello, una de las carencias más relevantes es la ausencia de marcos normativos que permitan a las autoridades atender la violencia digital sintética con precisión, ya que cuando el marco legal no distingue entre una imagen íntima real y una representación sintética generada por IA, las rutas institucionales tienden a operar con incertidumbre, se discute si encuadra o no en tipos existentes, se discute si “hay” o “no hay” hecho real, o se minimiza el daño bajo el argumento de que “no ocurrió”, desconociendo la naturaleza del *deepfake* y

²⁷Chesney y Citron, op. cit., p. 1772.

²⁸UN Women, “AI-powered online abuse,” 18 de noviembre de 2025, <https://www.unwomen.org/en/articles/faqs/ai-powered-online-abuse-how-ai-is-amplifying-violence-against-women-and-what-can-stop-it>

²⁹UN Women, How AI Is Exacerbating Technology-Facilitated Violence Against Women and Girls (UN Women, enero de 2026), <https://www.unwomen.org/sites/default/files/2026-01/how-ai-is-exacerbating-technology-facilitated-violence-against-women-and-girls-en.pdf>

trasladando a la víctima con una carga injusta, como lo es demostrar una falsedad que, para efectos sociales, ya está produciendo consecuencias³⁰.

Lo anterior cobra especial relevancia si se considera que los riesgos no se agotan en personas adultas, sino que la creación de imágenes sexualizadas sintéticas también involucran a niñas, niños y adolescentes, por ejemplo, mediante herramientas de “nudificación” u otras formas de manipulación, tan es así que ha sido señalado por la UNICEF, que los *deepfakes* son una amenaza creciente que exige respuestas normativas y de política pública, precisamente porque el daño se produce aunque el contenido sea sintético³¹. En fechas recientes, UNICEF también ha urgido a los Estados a criminalizar la creación de material de abuso sexual infantil generado por IA y fortalecer medidas de “seguridad desde el diseño”, ante reportes de crecimiento acelerado de este fenómeno³².

En ese sentido, el objetivo no es “regular la tecnología” en abstracto, sino establecer reglas claras frente a usos que generan riesgos inaceptables para las personas. En este punto resulta útil el enfoque de gestión de riesgos promovido por instituciones técnicas, como el NIST, que enfatiza la necesidad de identificar impactos negativos y fortalecer la confianza mediante prácticas responsables y de gobernanza a lo largo del ciclo de vida de los sistemas de IA³³.

En ese sentido, la presente propuesta de reforma busca atender un punto esencial, que es la brecha entre el daño y la respuesta de las autoridades, ya que un marco normativo adecuado debe permitir, en primer término, que las autoridades identifiquen con claridad la conducta y actúen sin ambigüedades; y, en segundo término, que la víctima cuente con rutas viables para protección y reparación, sin exponerse innecesariamente a revictimización.

³⁰ Jhordan Aguirre-Lanegra, Andherson y Ramos-Zaga, Fernando, “Deepfakes sexuales y violencia algorítmica: hacia un marco normativo integral de protección de la dignidad digital,” *Derecho a la Información*, 11, no. 21 (2026): e20198, DOI: <https://doi.org/10.22201/ij.25940082e.2026.21.20198> Disponible en: <https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/20198>

³¹ UNICEF, “Artificial intelligence and child sexual abuse and exploitation” (informe, 2026), <https://www.unicef.org/reports/artificial-intelligence-and-child-sexual-abuse-and-exploitation>

³² UNICEF, “‘Deepfake abuse is abuse’,” comunicado de prensa, 4 de febrero de 2026, <https://www.unicef.org/press-releases/deepfake-abuse-is-abuse>; ver también: Reuters, “UNICEF calls for criminalization of AI content depicting child sex abuse,” 5 de febrero de 2026, <https://www.reuters.com/legal/government/unicef-calls-criminalization-ai-content-depicting-child-sex-abuse-2026-02-05/>

³³ National Institute of Standards and Technology (NIST), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1 (2023), <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>

Dicho lo anterior, en el orden jurídico mexicano, durante los últimos años se han registrado avances relevantes en el reconocimiento de la violencia digital como una forma de agresión que afecta de manera directa la dignidad, la privacidad y la integridad de las personas; dichos avances se han materializado principalmente a través de reformas conocidas, como la “Ley Olimpia”, la cual incorporó, en diversos códigos penales, el reconocimiento de la difusión de contenido íntimo sin consentimiento como una conducta sancionable³⁴.

Estas reformas ayudaron en la visibilización y sanción de la violencia digital, al reconocer que la difusión de imágenes, audios o videos de carácter íntimo sin autorización genera daños y perjuicios en la vida de las personas afectadas. Asimismo, permitieron establecer que la violencia ejercida en entornos digitales puede tener consecuencias tan graves como aquellas que se materializan en el ámbito físico, especialmente cuando se trata de la exposición de la vida privada o de la sexualidad de las personas³⁵.

Asimismo, en el ámbito local, el Estado de Nuevo León también ha registrado mejoras relevantes en el reconocimiento de la violencia digital, particularmente a través de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia del Estado, la cual contempla dentro de sus disposiciones la utilización de tecnologías digitales, incluida la inteligencia artificial, para la creación o manipulación de imágenes, audios o videos de contenido íntimo sin consentimiento como una forma de violencia. Este reconocimiento permite establecer que la generación de contenidos sintéticos mediante inteligencia artificial puede constituir una conducta que vulnera la dignidad, la integridad y la seguridad de las personas, especialmente de las mujeres.

No obstante, aun cuando el marco normativo en materia de acceso de las mujeres a una vida libre de violencia ya reconoce estas conductas, resulta necesario armonizar el orden jurídico estatal para que dicho reconocimiento se traduzca en mecanismos claros de

³⁴Oropa, Marcela, et. al. *Informe Violencia Digital. Un estudio de los perfiles de agresores y sobrevivientes de violencia sexual digital*. Frente Nacional para la Sororidad y Defensoras Digitales, México 2022. Disponible en: [https://leyolimpia.com.mx/Docs/1%20-%20INFORME%20VIOLENCIA%20DIGITAL%20\(ME%CC%81XICO\)%20DICIEMBRE%202022.pdf](https://leyolimpia.com.mx/Docs/1%20-%20INFORME%20VIOLENCIA%20DIGITAL%20(ME%CC%81XICO)%20DICIEMBRE%202022.pdf)

³⁵ ONU Mujeres, *Violence against women in digital contexts* (New York: UN Women, 2022). Disponible en: <https://www.unwomen.org/en/digital-library/publications/2022/03/violence-against-women-in-digital-contexts>

sanción y reparación dentro de los ámbitos penal y civil. La falta de referencias específicas en estos ordenamientos puede generar dificultades en la persecución de las conductas, en la acreditación del daño y en la obtención de medidas efectivas de reparación para las víctimas.

En ese sentido, la presente iniciativa no parte de la inexistencia de regulación, sino de la necesidad de fortalecer y complementar el marco jurídico vigente mediante su armonización con las disposiciones ya contempladas en la Ley de Acceso de las Mujeres a una Vida Libre de Violencia del Estado de Nuevo León, a fin de asegurar coherencia normativa, certeza jurídica y una protección integral frente a nuevas formas de violencia digital vinculadas al uso indebido de la inteligencia artificial.

De manera que, ante el surgimiento y expansión de tecnologías de inteligencia artificial, capaces de generar contenidos falsos, se plantea un desafío adicional que no se encontraba plenamente previsto al momento de diseñar dichas reformas, pues, mientras la normativa vigente se enfoca principalmente en la difusión de material íntimo real obtenido sin consentimiento, el fenómeno de los *deepfakes* introduce la posibilidad de crear representaciones completamente falsas que simulan la identidad y el cuerpo de una persona, generando afectaciones equiparables o incluso más complejas que las previstas originalmente por el legislador.

En ese sentido, el marco normativo actual presenta limitaciones para abordar de manera integral las conductas relacionadas con la utilización de la IA para la creación y difusión de contenidos íntimos; la ausencia de una referencia expresa a materiales generados mediante inteligencia artificial, puede generar incertidumbre sobre la tipificación de las conductas, la competencia de las autoridades o los mecanismos de reparación disponibles para las víctimas³⁶. Ahora bien, ello no implica desconocer el progreso logrado en materia de violencia digital, sino reconocer que el desarrollo tecnológico ha superado la capacidad de respuesta de las normas existentes.

Además, las rutas institucionales disponibles suelen centrarse en la sanción penal de la difusión de contenido íntimo, sin contemplar de manera suficiente otras dimensiones del daño que producen los *deepfakes*, como la afectación reputacional, el impacto en la vida

³⁶Aguirre-Lanegra y Ramos-Zaga, op. cit., p. 10.

laboral, la utilización del material con fines de extorsión o la permanencia del contenido en entornos digitales incluso después de su eliminación inicial.

Por su parte, reconocer estos vacíos, no implica desestimar la importancia de las reformas existentes, sino consolidarlas y actualizarlas frente a un contexto tecnológico en constante transformación, por eso, la regulación de la violencia digital no puede permanecer estática cuando las herramientas utilizadas para ejercerla evolucionan de forma acelerada; por el contrario, el derecho debe adaptarse para garantizar que la protección de la dignidad, la intimidad y la integridad personal se mantenga efectiva también frente a las nuevas formas de agresión facilitadas por la inteligencia artificial³⁷.

En ese sentido, el fenómeno de los contenidos generados con IA evidencian una brecha creciente entre la velocidad de la innovación tecnológica, y la capacidad de adaptación de los marcos normativos vigentes, pues mientras que las herramientas de generación de imagen y video con IA se han vuelto más accesibles, sofisticadas y difíciles de detectar, los marcos legales existentes continúan basándose, en gran medida, en la existencia de hechos materiales verificables o en la difusión de contenidos auténticos obtenidos sin consentimiento³⁸.

En este sentido, la evolución tecnológica ha generado un escenario en el que determinadas conductas altamente lesivas pueden no encuadrar de manera clara en las figuras existentes o hacerlo de forma indirecta, obligando a interpretaciones extensivas que generan incertidumbre tanto para las víctimas como para las autoridades encargadas de la procuración de justicia. En consecuencia, la falta de referencias específicas en la legislación penal y civil respecto de la creación y difusión de contenidos íntimos sintéticos puede derivar en dilación en la atención de los casos, dificultades para acreditar el daño o limitaciones para garantizar una reparación integral, particularmente cuando el material es completamente fabricado pero socialmente percibido como real.

En ese contexto, uno de los principales desafíos radica en la dificultad para reparar el daño una vez que el contenido ha sido generado y difundido, pues, a diferencia de otros ilícitos, los *deepfakes* pueden reproducirse indefinidamente y mantenerse en circulación incluso

³⁷ UNESCO, Recommendation on the Ethics of Artificial Intelligence (Paris: UNESCO, 2021), <https://unesdoc.unesco.org/ark:/48223/pf0000380455>

³⁸ Chesney y Citron, op. cit., pp. 1786-1791.

después de haberse eliminado de su fuente original, lo que genera una afectación prolongada en la vida de las víctimas, quienes pueden enfrentar consecuencias personales, profesionales y sociales de larga duración, así como una sensación persistente de vulnerabilidad³⁹.

En el ámbito local, el Estado de Nuevo León cuenta con condiciones institucionales, tecnológicas y sociales que lo colocan en una posición estratégica para impulsar respuestas normativas innovadoras frente a los desafíos que plantea la inteligencia artificial. La alta conectividad digital, la presencia de sectores tecnológicos en crecimiento y la intensa interacción social en entornos digitales convierten a la entidad en un espacio donde los beneficios de la innovación conviven con riesgos emergentes que requieren atención legislativa oportuna.⁴⁰

En consecuencia, el desarrollo de un marco normativo que reconozca y atienda la violencia digital sintética no sólo responde a una necesidad actual, sino que posiciona al Estado como un referente en la protección de derechos frente a tecnologías emergentes. La adopción de medidas legislativas claras permitirá dotar de mayor certeza jurídica a las autoridades, fortalecer la confianza ciudadana en las instituciones y enviar un mensaje inequívoco de que la dignidad, la identidad y la vida privada de las personas deben ser protegidas también en los entornos digitales y sintéticos⁴¹.

En este contexto, resulta necesario que el derecho evolucione de manera paralela al desarrollo tecnológico, particularmente cuando las herramientas emergentes tienen la capacidad de generar impactos directos en la dignidad, la identidad y la vida privada de las personas. La expansión de la inteligencia artificial ha ampliado las posibilidades de creación y difusión de contenidos, pero también ha abierto espacios para la materialización de conductas que pueden afectar gravemente a quienes son objeto de representaciones sintéticas no consensuadas. Frente a ello, la actualización del marco jurídico se presenta como una medida necesaria para garantizar que la protección de los derechos fundamentales se mantenga efectiva en los entornos digitales contemporáneos.

³⁹ Chesney y Citron, op. cit., pp. 1771-1779.

⁴⁰ OECD. Artificial Intelligence in Society. OECD Publishing, 2019.

⁴¹ UN Women. Violence against women in digital contexts. 2022.

La intervención normativa que se propone no busca limitar el desarrollo tecnológico ni restringir el ejercicio legítimo de la libertad de expresión, sino establecer límites claros frente a usos que vulneran la dignidad humana, la privacidad y la integridad personal. Por lo que, reconocer jurídicamente la violencia digital sintética permitiría fortalecer el marco de protección existente, dotar de mayor certeza a las autoridades y brindar a las personas afectadas mecanismos más claros de atención y reparación.

Asimismo, la actualización del marco jurídico local representa una oportunidad para que el Estado de Nuevo León consolide una respuesta preventiva y acorde con los desafíos que plantea la inteligencia artificial. La adopción de disposiciones específicas en esta materia contribuirá a cerrar brechas de protección, anticipar riesgos y garantizar que el desarrollo tecnológico se mantenga dentro de parámetros compatibles con el respeto a los derechos fundamentales.

En consecuencia, el objetivo de la presente es fortalecer la protección de la dignidad, la identidad y la vida privada de las personas frente a nuevas formas de violencia digital, reconociendo que la innovación tecnológica debe ir acompañada de mecanismos jurídicos que aseguren un entorno digital seguro, respetuoso y acorde con los principios fundamentales que rigen nuestro orden jurídico.

Por último, cabe destacar que en el ámbito penal, el Estado de Nuevo León ha incorporado recientemente referencias al uso de tecnologías digitales en la comisión de conductas que vulneran la intimidad y la integridad de las personas, lo que representa un avance relevante en el reconocimiento de nuevas formas de violencia vinculadas al entorno digital.

No obstante, la evolución acelerada de las herramientas de inteligencia artificial y su capacidad para generar o manipular contenidos íntimos con alto grado de realismo ha evidenciado la necesidad de contar con disposiciones más claras, específicas y sistemáticas que permitan atender de manera integral estas conductas. La regulación vigente, si bien constituye un paso inicial, no desarrolla de forma expresa los alcances, supuestos y consecuencias jurídicas asociados a la creación y utilización de contenidos sintéticos íntimos, lo que puede generar zonas de incertidumbre en su interpretación y aplicación.

En ese sentido, la presente iniciativa tiene como finalidad fortalecer y precisar el marco jurídico estatal, a fin de cerrar dichas brechas y garantizar una respuesta normativa más clara, coherente y efectiva frente a esta modalidad emergente de violencia digital.

Por lo anteriormente expuesto y fundado, se agrega un cuadro comparativo de la propuesta de reforma de la siguiente forma:

CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN CAPÍTULO IV DELITOS CONTRA LA INTIMIDAD SEXUAL	
Texto vigente	Texto propuesto
ARTÍCULO 271 BIS 5.- COMETE EL DELITO CONTRA LA INTIMIDAD PERSONAL, QUIEN O QUIENES, REVELEN, DIFUNDAN, DISTRIBUYAN, PUBLIQUEN O EXHIBAN MEDIANTE CORREO ELECTRÓNICO, MENSAJES TELEFÓNICOS, REDES SOCIALES O POR CUALQUIER OTRO MEDIO, IMÁGENES, AUDIOS O VIDEOS DE CONTENIDO ERÓTICO, SEXUAL O PORNOGRÁFICO AUTÉNTICO O ALTERADO A TRAVÉS DE MEDIOS DIGITALES, DE UNA PERSONA SIN SU CONSENTIMIENTO.	ARTÍCULO 271 BIS 5.- COMETE EL DELITO CONTRA LA INTIMIDAD PERSONAL QUIEN O QUIENES REVELEN, DIFUNDAN, DISTRIBUYAN, PUBLIQUEN, EXHIBAN, COMPARTAN, TRANSMITAN, COMERCIALICEN O PONGAN A DISPOSICIÓN DE TERCEROS , MEDIANTE CORREO ELECTRÓNICO, MENSAJERÍA TELEFÓNICA , REDES SOCIALES O POR CUALQUIER OTRO MEDIO DIGITAL O FÍSICO , IMÁGENES, AUDIOS O VIDEOS DE CONTENIDO ERÓTICO, SEXUAL O PORNOGRÁFICO AUTÉNTICO, SIMULADO O ALTERADO, INCLUSO AQUELLOS CREADOS, GENERADOS, MODIFICADOS O MANIPULADOS MEDIANTE INTELIGENCIA ARTIFICIAL, ALGORITMOS O CUALQUIER TECNOLOGÍA DIGITAL , DE UNA PERSONA SIN SU CONSENTIMIENTO.
ASÍ COMO QUIEN VIDEOGRABE, AUDIOGRABE, FOTOGRAFÍE, IMPRIMA, ELABORE, GENERE O ALTERE, IMÁGENES, AUDIOS O VIDEOS CON CONTENIDO ÍNTIMO SEXUAL DE UNA PERSONA SIN SU CONSENTIMIENTO.	
A QUIEN COMETA EL DELITO DESCRITO EN LOS PÁRRAFOS ANTERIORES, SE LE	ASÍ COMO A QUIEN VIDEOGRABE, AUDIOGRABE, FOTOGRAFÍE, IMPRIMA,

IMPONDRÁ UNA PENA DE TRES A SEIS AÑOS DE PRISIÓN. LA PENA SE AUMENTARÁ HASTA EN UNA MITAD: I. CUANDO LAS IMÁGENES, AUDIO O VIDEOS DE CONTENIDO EROTICO, SEXUAL O PORNOGRÁFICO HAYAN SIDO OBTENIDOS CUANDO LA VÍCTIMA FUESE MENOR DE DIECIOCHO AÑOS DE EDAD, O BIEN, CUANDO NO TENGA LA CAPACIDAD DE COMPRENDER O RESISTIR EL CARÁCTER ERÓTICO, SEXUAL O PORNOGRÁFICO DEL HECHO QUE CONSTITUYE EL CONTENIDO REVELADO, DIFUNDIDO, PUBLICADO O EXHIBIDO; II. a VI. ... [SIN CORRELATIVO]	ELABORE, GENE, SIMULE, ALTERE, PRODUZCA O MODIFIQUE, MEDIANTE EL USO DE INTELIGENCIA ARTIFICIAL GENERATIVA O CUALQUIER SOFTWARE DE MANIPULACIÓN DIGITAL, IMÁGENES, AUDIOS O VIDEOS CON CONTENIDO ÍNTIMO O SEXUAL DE UNA PERSONA SIN SU CONSENTIMIENTO, CUANDO DICHO MATERIAL SEA SUSCEPTIBLE DE GENERAR APARIENCIA DE AUTENTICIDAD, RAZONABLEMENTE INDUZCA A ERROR O SE PRESENTE COMO REAL O VERDADERO. SE PRESUMIRÁ LA EXISTENCIA DE DOLO CUANDO CONCURRAN LOS ELEMENTOS OBJETIVOS CONSISTENTES EN: I. LA AUSENCIA DE CONSENTIMIENTO EXPRESO, ESPECÍFICO E INEQUÍVOCO DE LA PERSONA AFECTADA; II. EL USO DE INTELIGENCIA ARTIFICIAL GENERATIVA O SOFTWARE DE MANIPULACIÓN DIGITAL; Y III. LA PRODUCCIÓN DE UN MATERIAL SUSCEPTIBLE DE GENERAR APARIENCIA DE AUTENTICIDAD O INDUCIR A ERROR RESPECTO DE LA PERSONA REPRESENTADA. A QUIEN COMETA EL DELITO DESCRITO EN LOS PÁRRAFOS ANTERIORES, SE LE
---	---

	IMPONDRÁ UNA PENA DE TRES A SEIS AÑOS DE PRISIÓN. LA PENA SE AUMENTARÁ HASTA EN UNA MITAD: I. CUANDO LAS IMÁGENES, AUDIOS O VIDEOS DE CONTENIDO ERÓTICO, SEXUAL O PORNOGRÁFICO HAYAN SIDO OBTENIDOS, GENERADOS, PRODUCIDOS, MANIPULADOS, ALTERADOS O COMPARTIDOS, CUANDO LA VÍCTIMA FUESE MENOR DE DIECIOCHO AÑOS DE EDAD; O BIEN, CUANDO ÉSTA NO TENGA LA CAPACIDAD DE COMPRENDER O RESISTIR EL CARÁCTER ERÓTICO, SEXUAL O PORNOGRÁFICO DEL HECHO QUE CONSTITUYE EL CONTENIDO REVELADO, DIFUNDIDO, PUBLICADO O EXHIBIDO; II. a VI. ... VII. CUANDO LA CONDUCTA TENGA COMO FINALIDAD DAÑAR LA REPUTACIÓN, EL HONOR O LA IMAGEN PÚBLICA DE LA VÍCTIMA MEDIANTE EL USO DE CONTENIDO SIMULADO O FALSO.
--	---

CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN	
CAPÍTULO V	
DE LAS OBLIGACIONES QUE NACEN DE LOS ACTOS ILICITOS	
Texto vigente	Texto propuesto

[SIN CORRELATIVO]	Artículo 1813 Bis IV. También procederá la indemnización por reparación moral o daño moral a que se refieren los artículos 1813 y 1813 bis de este Código cuando se origine por la creación, alteración, edición, generación, difusión, comercialización, transmisión o puesta a disposición de contenido de carácter íntimo sexual, real o simulado, generado o manipulado mediante sistemas automatizados o inteligencia artificial, cuando: I. La persona afectada sea identificable, directa o indirectamente; y II. No exista consentimiento expreso, específico e inequívoco para la generación y/o la difusión del contenido. Para la cuantificación de la indemnización y las modalidades de la reparación del daño, se estará a lo dispuesto por el artículo 1813 y 1813 bis de este código.
[SIN CORRELATIVO]	Artículo 1813 Bis V. En las acciones relativas a la creación, alteración, edición, generación, difusión, comercialización, transmisión o puesta a disposición del contenido de carácter íntimo sexual, real o simulado, generado o manipulado mediante sistemas automatizados o inteligencia artificial, en términos del artículo 1813 Bis IV, el juez que conozca

	del asunto, a solicitud de la parte interesada, podrá otorgar las siguientes medidas de protección: I. Retiro, eliminación o deshabilitación del acceso al contenido ya difundido, cuando se encuentre bajo el control, administración o posibilidad de gestión del agresor, así como abstención de su reproducción o nueva difusión, sin perjuicio de la preservación de evidencia digital. II. Requerimiento a las plataformas digitales, redes sociales, páginas de internet o servicios de alojamiento o difusión de contenido para la eliminación, bloqueo o deshabilitación del acceso al contenido, identificado mediante enlace, dirección electrónica, usuario, perfil, URL u otro dato técnico de localización.
[SIN CORRELATIVO]	Artículo 1813 Bis VI. Incurrirán en responsabilidad civil las plataformas digitales, aplicaciones, sistemas de inteligencia artificial o proveedores de servicios tecnológicos que permitan la generación, edición o difusión de imágenes, audios o videos, cuando por omisión negligente en la implementación de medidas razonables de seguridad faciliten la creación o circulación de contenido íntimo o sexual no consentido de personas identificables.

	Se entenderá que existe omisión negligente cuando, conforme al estado de la técnica, resulte razonablemente exigible la adopción de mecanismos de prevención, detección o bloqueo de este tipo de contenido y éstos no hubiesen sido implementados o resulten notoriamente insuficientes, y la plataforma o proveedor haya sido notificado del contenido sin adoptar medidas diligentes para impedir su continuidad o propagación.
--	---

CÓDIGO DE PROCEDIMIENTOS CIVILES DEL ESTADO DE NUEVO LEÓN CAPÍTULO VI DE LAS ÓRDENES DE PROTECCIÓN	
Texto vigente	Texto propuesto
[SIN CORRELATIVO]	Artículo 222 Bis XIII. Para el trámite de las órdenes de protección a que se refiere el artículo 1813 Bis V, del Código Civil para el Estado de Nuevo León, se estará a lo dispuesto en los artículos 222 Bis I, 222 Bis II, 222 Bis III y 222 Bis X del presente Código. Serán competentes para conocer y resolver dichas solicitudes los jueces en materia civil. Cuando por razones de urgencia no sea posible acudir ante el juez civil competente, el juez del lugar donde se presente la solicitud deberá admitirla y pronunciarse de inmediato sobre la

	procedencia de las medidas, sin que pueda negarse a conocer por razón de competencia. Una vez dictadas y ejecutadas las órdenes de protección, remitirá las actuaciones al juez civil competente.
--	---

Derivado de lo anterior, se somete a consideración la siguiente iniciativa con proyecto de:

DECRETO

POR EL QUE SE REFORMAN DIVERSAS DISPOSICIONES AL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN, EL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN Y EL CÓDIGO DE PROCEDIMIENTOS CIVILES DEL ESTADO DE NUEVO LEÓN, AL TENOR DE LA SIGUIENTE:

PRIMERO.- SE REFORMA EL ARTÍCULO 271 BIS 5 DEL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN, PARA QUEDAR COMO SIGUE:

ARTÍCULO 271 BIS 5.- COMETE EL DELITO CONTRA LA INTIMIDAD PERSONAL QUIEN O QUIENES REVELEN, DIFUNDAN, DISTRIBUYAN, PUBLIQUEN, EXHIBAN, COMPARTAN, TRANSMITAN, COMERCIALICEN O PONGAN A DISPOSICIÓN DE TERCEROS, MEDIANTE CORREO ELECTRÓNICO, MENSAJERÍA TELEFÓNICA, REDES SOCIALES O POR CUALQUIER OTRO MEDIO DIGITAL O FÍSICO, IMÁGENES, AUDIOS O VIDEOS DE CONTENIDO ERÓTICO, SEXUAL O PORNOGRÁFICO AUTÉNTICO, SIMULADO O ALTERADO, INCLUSO AQUELLOS CREADOS, GENERADOS, MODIFICADOS O MANIPULADOS MEDIANTE INTELIGENCIA ARTIFICIAL, ALGORITMOS O CUALQUIER TECNOLOGÍA DIGITAL, DE UNA PERSONA SIN SU CONSENTIMIENTO.

ASÍ COMO A QUIEN VIDEOGRABE, AUDIOGRABE, FOTOGRAFÍE, IMPRIMA, ELABORE, GENERE, SIMULE, ALTERE, PRODUZCA O MODIFIQUE, MEDIANTE EL USO DE INTELIGENCIA ARTIFICIAL GENERATIVA O CUALQUIER SOFTWARE DE MANIPULACIÓN DIGITAL, IMÁGENES, AUDIOS O VIDEOS CON CONTENIDO ÍNTIMO O

SEXUAL DE UNA PERSONA SIN SU CONSENTIMIENTO, CUANDO DICHO MATERIAL SEA SUSCEPTIBLE DE GENERAR APARIENCIA DE AUTENTICIDAD, RAZONABLEMENTE INDUZCA A ERROR O SE PRESENTE COMO REAL O VERDADERO.

SE PRESUMIRÁ LA EXISTENCIA DE DOLO CUANDO CONCURRAN LOS ELEMENTOS OBJETIVOS CONSISTENTES EN:

I. LA AUSENCIA DE CONSENTIMIENTO EXPRESO, ESPECÍFICO E INEQUÍVOCO DE LA PERSONA AFECTADA;

II. EL USO DE INTELIGENCIA ARTIFICIAL GENERATIVA O SOFTWARE DE MANIPULACIÓN DIGITAL; Y

III. LA PRODUCCIÓN DE UN MATERIAL SUSCEPTIBLE DE GENERAR APARIENCIA DE AUTENTICIDAD O INDUCIR A ERROR RESPECTO DE LA PERSONA REPRESENTADA.

A QUIEN COMETA EL DELITO DESCRITO EN LOS PÁRRAFOS ANTERIORES, SE LE IMPONDRÁ UNA PENA DE TRES A SEIS AÑOS DE PRISIÓN.

LA PENA SE AUMENTARÁ HASTA EN UNA MITAD:

I. CUANDO LAS IMÁGENES, AUDIOS O VIDEOS DE CONTENIDO ERÓTICO, SEXUAL O PORNOGRÁFICO HAYAN SIDO OBTENIDOS, GENERADOS, PRODUCIDOS, MANIPULADOS, ALTERADOS O COMPARTIDOS, CUANDO LA VÍCTIMA FUESE MENOR DE DIECIOCHO AÑOS DE EDAD; O BIEN, CUANDO ÉSTA NO TENGA LA CAPACIDAD DE COMPRENDER O RESISTIR EL CARÁCTER ERÓTICO, SEXUAL O PORNOGRÁFICO DEL HECHO QUE CONSTITUYE EL CONTENIDO REVELADO, DIFUNDIDO, PUBLICADO O EXHIBIDO;

II. a VI. ...

VII. CUANDO LA CONDUCTA TENGA COMO FINALIDAD DAÑAR LA REPUTACIÓN, EL HONOR O LA IMAGEN PÚBLICA DE LA VÍCTIMA MEDIANTE EL USO DE CONTENIDO SIMULADO O FALSO.

SEGUNDO.- SE ADICIONA EL ARTÍCULO 1813 BIS IV AL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN, PARA QUEDAR COMO SIGUE:

Artículo 1813 Bis IV. También procederá la indemnización por reparación moral o daño moral a que se refieren los artículos 1813 y 1813 bis de este Código cuando se origine por la creación, alteración, edición, generación, difusión, comercialización, transmisión o puesta a disposición de contenido de carácter íntimo sexual, real o simulado, generado o manipulado mediante sistemas automatizados o inteligencia artificial, cuando:

- I. La persona afectada sea identificable, directa o indirectamente; y
- II. No exista consentimiento expreso, específico e inequívoco para la generación y/o la difusión del contenido.

Para la cuantificación de la indemnización y las modalidades de la reparación del daño, se estará a lo dispuesto por el artículo 1813 y 1813 bis de este código.

TERCERO.- SE ADICIONA EL ARTÍCULO 1813 BIS V AL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN, PARA QUEDAR COMO SIGUE:

Artículo 1813 Bis V. En las acciones relativas a la creación, alteración, edición, generación, difusión, comercialización, transmisión o puesta a disposición del contenido de carácter íntimo sexual, real o simulado, generado o manipulado mediante sistemas automatizados o inteligencia artificial, en términos del artículo 1813 Bis IV, el juez que conozca del asunto, a solicitud de la parte interesada, podrá otorgar las siguientes medidas de protección:

- I. Retiro, eliminación o deshabilitación del acceso al contenido ya difundido, cuando se encuentre bajo el control, administración o posibilidad de gestión del agresor, así como abstención de su reproducción o nueva difusión, sin perjuicio de la preservación de evidencia digital.

II. Requerimiento a las plataformas digitales, redes sociales, páginas de internet o servicios de alojamiento o difusión de contenido para la eliminación, bloqueo o deshabilitación del acceso al contenido, identificado mediante enlace, dirección electrónica, usuario, perfil, URL u otro dato técnico de localización.

CUARTO.- SE ADICIONA EL ARTÍCULO 1813 BIS VI AL CÓDIGO CIVIL PARA EL ESTADO DE NUEVO LEÓN.

Artículo 1813 Bis VI. También incurrirán en responsabilidad civil las plataformas digitales, aplicaciones, sistemas de inteligencia artificial o proveedores de servicios tecnológicos que permitan la generación, edición o difusión de imágenes, audios o videos, cuando por omisión negligente en la implementación de medidas razonables de seguridad faciliten la creación o circulación de contenido íntimo o sexual no consentido de personas identificables.

Se entenderá que existe omisión negligente cuando, conforme al estado de la técnica, resulte razonablemente exigible la adopción de mecanismos de prevención, detección o bloqueo de este tipo de contenido y éstos no hubiesen sido implementados o resulten notoriamente insuficientes, y la plataforma o proveedor haya sido notificado del contenido sin adoptar medidas diligentes para impedir su continuidad o propagación.

QUINTO.- SE ADICIONA EL ARTÍCULO 222 BIS XIII AL CÓDIGO DE PROCEDIMIENTOS CIVILES DEL ESTADO DE NUEVO LEÓN, PARA QUEDAR COMOS SIGUE:

Artículo 222 Bis XIII. Para el trámite de las órdenes de protección a que se refiere el artículo 323 Bis 7, fracciones VI y VII, del Código Civil para el Estado de Nuevo León, se estará a lo dispuesto en los artículos 222 Bis I, 222 Bis II, 222 Bis III y 222 Bis X del presente Código.

Serán competentes para conocer y resolver dichas solicitudes los jueces en materia civil. Cuando por razones de urgencia no sea posible acudir ante el juez civil competente, el juez del lugar donde se presente la solicitud deberá admitirla y pronunciarse de inmediato sobre la procedencia de las medidas, sin que pueda negarse a conocer por razón de competencia.

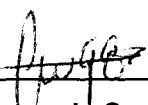
Una vez dictadas y ejecutadas las órdenes de protección, remitirá las actuaciones al juez civil competente.

TRANSITORIOS. –

PRIMERO. El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Estado de Nuevo León.

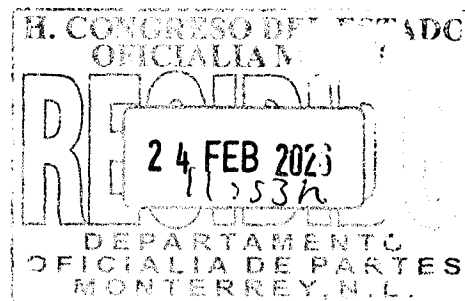
SEGUNDO. La Fiscalía General de Justicia del Estado de Nuevo León deberá, dentro de los ciento ochenta días naturales siguientes a la entrada en vigor del presente Decreto, realizar las adecuaciones correspondientes a su Reglamento Interno, a efecto de crear una unidad administrativa subalterna adscrita a la Vicefiscalía del Ministerio Público, con competencia específica para la atención, investigación, preservación, certificación expedita de evidencia digital y demás actuaciones ministeriales vinculadas con las conductas previstas en el artículo 271 Bis 5 del Código Penal y con las medidas de protección previstas en el artículo 1813 Bis V del Código Civil, en términos de la presente iniciativa, privilegiando la atención urgente, la debida diligencia y la no revictimización.

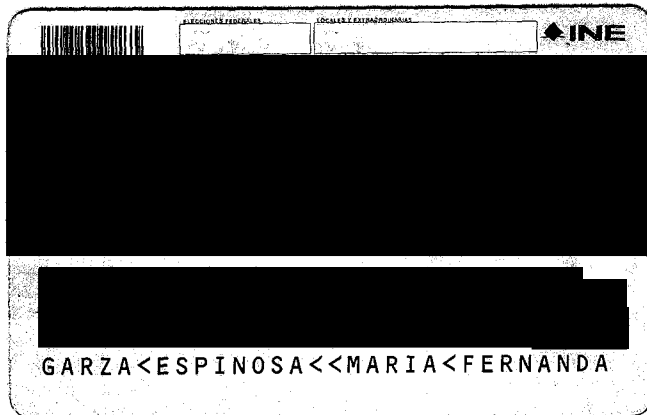
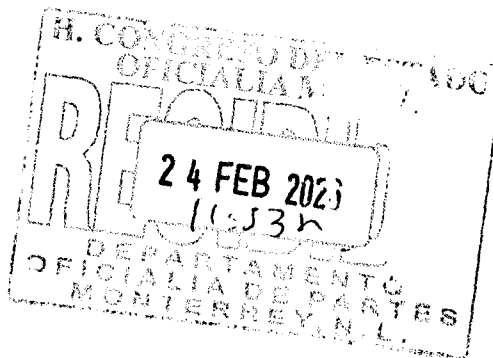
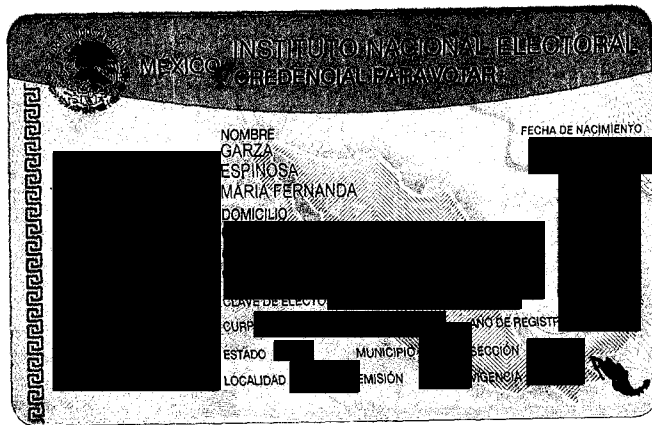
Monterrey, Nuevo León, a XX de enero de 2026.

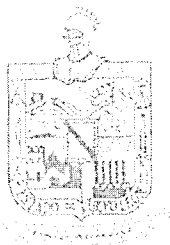


María Fernanda Garza Espinosa

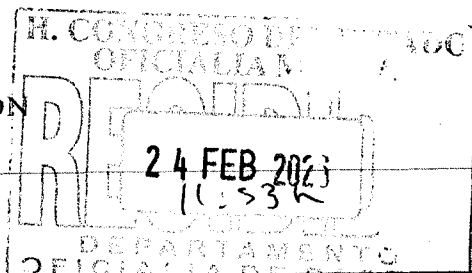
Integrante de la Asociación Civil denominada “Fundación Duque para el Apoyo de la Familia y las Artes”.







H. CONGRESO DEL ESTADO DE NUEVO LEÓN
LXXVII LEGISLATURA
OFICIALÍA DE PARTES



AVISO DE PRIVACIDAD SIMPLIFICADO

El H. Congreso del Estado de Nuevo León, es el responsable del tratamiento de los datos personales que nos proporcione.

Finalidades para las cuales serán tratados sus Datos Personales

Sus datos personales serán utilizados para: a) Registro de Iniciativas; b) Registro de Convocatorias. (Otros documentos o información que consideren se presentan); y c) Trámites, asuntos administrativos. Los datos personales recabados serán protegidos, incorporados y tratados en la Oficialía de Partes, adscrita a la Oficialía Mayor de este H. Congreso del Estado.

Transferencia de Datos

Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

Mecanismos para el ejercicio de los derechos ARCO

Se informa que podrá ejercer sus derechos de Acceso, Rectificación, Cancelación u Oposición (ARCO) de sus datos personales de forma presencial ante la Unidad de Transparencia del H. Congreso del Estado, a través de la Plataforma Nacional de Transparencia (<http://www.plataformadetransparencia.org.mx/>), o al correo electrónico enlace.transparencia@hcnl.gob.mx. Si desea conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia a la dirección antes señalada, enviar un correo electrónico a enlace.transparencia@hcnl.gob.mx o bien, comunicarse al Tel: 81815-095000 ext. 1065.



Sitio dónde consultar el Aviso de Privacidad Integral

Usted podrá consultar el Aviso de Privacidad Integral en la siguiente dirección electrónica: <https://www.hcnl.gob.mx/privacidad/> o bien, de manera presencial en las instalaciones del Congreso del Estado, directamente en la Unidad de Transparencia.

Última actualización: Febrero 2025

Consiento y autorizo que mis datos personales y datos sensibles (si se presenta el caso) sean tratados conforme a lo previsto en el presente aviso de privacidad.

Si autorizo



No autorizo



Domicilio para recibir las notificaciones que correspondan:

Calle:



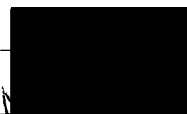
Núm. Ext.



Núm. Int.

Colonia:

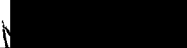
Municipio:



Teléfono(s):



Estado:



C.P.



Consiento y autorizo el recibir las notificaciones a través de medios electrónicos; y en su caso, señalo el siguiente correo electrónico.

Si autorizo



No autorizo



Correo:



NOMBRE Y FIRMA AUTÓGRAFA DEL INTERESADO