INICIATIVA QUE REFORMA EL TÍTULO VIGÉSIMO DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE VIOLENCIA DIGITAL Y LOS DELITOS DERIVADOS DEL USO DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN, LA INFORMACIÓN Y LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL, A CARGO DEL DIPUTADO RICARDO MONREAL ÁVILA, DEL GRUPO PARLAMENTARIO DE MORENA

El suscrito, doctor Ricardo Monreal Ávila, diputado integrante y coordinador del Grupo Parlamentario de Morena en esta LXVI Legislatura del Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72 de la Constitución Política de los Estados Unidos Mexicanos, y en los artículos 6, numeral 1, fracción I, y 77 del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente **iniciativa con proyecto de decreto por el que se reforma el Título Vigésimo del Código Penal Federal, en materia de violencia digital y los delitos derivados del uso de las tecnologías de la comunicación, la información y los sistemas de inteligencia artificial,** al tenor de la siguiente.

Exposición de Motivos

En la actualidad, el desarrollo tecnológico ha dado lugar a una profunda transformación en la manera en que las personas interactúan, acceden a la información y realizan actividades económicas, sociales y políticas. Las tecnologías de la información y la comunicación (TIC), así como los sistemas de inteligencia artificial (IA), han revolucionado la vida cotidiana y han generado beneficios incalculables en múltiples sectores. Sin embargo, el uso indebido de los avances tecnológicos de nuestra época también ha propiciado la comisión de nuevas formas de conductas ilícitas que vulneran derechos fundamentales, la seguridad de las personas e incluso la estabilidad de las instituciones del Estado.

La creciente incidencia de los delitos cibernéticos exige una respuesta legislativa adecuada que garantice la protección de las personas en el entorno digital, en especial si se considera la afectación inmediata que producen en detrimento de la integridad de las personas, sobre todo por la rapidez con la que se difunden los contenidos digitales a través de la banda ancha y el Internet, como consecuencia de la llamada “viralización” que se produce sobre todo en redes sociales o medios digitales, sin que en medie un mínimo de rigor ético, moral y mucho menos jurídico en cuanto a su generación y transmisión.

De hecho, en febrero de 2025 la Secretaría de Gobernación (SEGOB) presentó el *Diagnóstico sobre delitos cibernéticos en la legislación penal del país,* en el que se identificaron las conductas ilícitas identificadas como “delitos cibernéticos” y su tipificación en el Código Penal Federal, así como en la legislación penal de las 32 Entidades Federativas. De este estudio se destaca la existencia de 9 delitos cibernéticos, tales como: espionaje; ataques a las vías de comunicación; revelación de secretos; acceso ilícito a sistemas y equipos de informática; delitos en materia de derechos de autor; comunicación de contenido sexual con personas menores de dieciocho años; corrupción de personas menores de dieciocho años; pornografía de personas menores de dieciocho años; y otros relacionados en contra de niñas, niños y adolescentes.

No obstante, la existencia de la tipificación de algunos delitos cibernéticos dentro del Código Penal Federal, persiste una omisión legislativa significativa: desde el 1 de junio de 2021 el Congreso de la Unión no ha incorporado a la legislación penal federal la figura de "violencia digital",[1] tal como se estableció en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia. Esta laguna jurídica se torna más preocupante ante la irrupción y sofisticación de los sistemas de inteligencia artificial (IA), que han ampliado las modalidades y alcances de los delitos cibernéticos.

En efecto, el Código Penal Federal vigente no contempla de manera específica todas las conductas delictivas derivadas del uso indebido de las TIC y la IA, lo que genera vacíos normativos que dificultan la persecución y sanción de estos delitos. Ante esta situación, resulta imprescindible adecuar el marco jurídico penal para tipificar y sancionar estas conductas con el fin de garantizar la protección de los derechos de las personas y la seguridad en el entorno digital, en especial si se considera la irrupción y sofisticación de los sistemas de IA y los desafíos que abre para la sociedad en los tiempos actuales.

La usurpación de identidad digital, la manipulación de información ya sea imágenes, audios o videos reales o simulados, a través del uso de los sistemas de IA, la creación y difusión de desinformación automatizada a través de la Internet, así como la utilización de algoritmos con fines delictivos, son algunos de los principales actos que afectan tanto a particulares como a instituciones públicas y privadas, generando daños económicos, afectaciones a la privacidad e incluso riesgos a la seguridad nacional.

Desde hace al menos veinticuatro años, instrumentos internacionales como la Convención de Budapest sobre Ciberdelincuencia han reconocido la necesidad de legislar en materia de delitos cibernéticos y de optar por la cooperación internacional en su combate, dado que las fronteras territoriales hoy se han desdibujado a partir del uso de las TIC, específicamente de la banda ancha y el Internet.[2]

Y aunque se ha avanzado en la materia, los avances tecnológicos han sido mucho mayores y cada vez más sofisticados. De hecho, en noviembre de 2021 la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) adoptó la primera norma mundial sobre la ética de la IA, denominada "Recomendación sobre la Ética de la Inteligencia Artificial" en el marco de la 41ª. Conferencia General de la UNESCO, como un instrumento internacional que enfatiza la importancia de regular el uso de la IA para prevenir abusos y garantizar su uso responsable.[3]

Los beneficios del uso de la IA en la vida cotidiana son numerosos y se vendrán multiplicando en la medida de que su aplicación se realice en ámbitos como la medicina y la ingeniería. Sin embargo, su uso indebido ha facilitado la creación de contenidos falsos, como *deepfakes* [4] que pueden ser utilizados para el ciberbullying, el ciberacoso, la difamación y otras formas de violencia digital. La dificultad para distinguir entre imágenes reales y manipuladas se ha incrementado con el uso de IA, especialmente en contextos sociales sensibles.

Uno de los riesgos más preocupantes es la alteración de imágenes, sonidos o videos con el propósito de difundir información falsa o comprometedora sobre una persona, afectando su reputación y generando consecuencias legales y sociales graves. En México, casos de *deepfakes* han sido utilizados para desacreditar a personas públicas y para realizar extorsiones, lo que demuestra la urgencia de legislar sobre este fenómeno. El acceso a herramientas de IA que permiten manipular contenido de manera cada vez más realista ha multiplicado el impacto de estas agresiones, dificultando la identificación de los responsables y la reparación del daño a las víctimas.

Si a esta problemática se suma otro tipo de conductas cibernéticas perjudiciales como son el *ciberacoso* y el *cyberbullying* que afectan principalmente a niñas, niños y adolescentes, encontramos que el Congreso de la Unión debe legislar en torno a la violencia digital con un enfoque integral, no sólo que garantice la libertad de expresión e ideas como derechos fundamentales de las y los mexicanos, sino también límites claros para aquellos que haciendo uso de las TIC y los sistemas de IA pretendan dañar la integridad de las personas.

Datos oficiales del Fondo de las Naciones Unidas para la Infancia (UNICEF) de 2019, advertían que entonces 1 de cada 3 niños en el mundo había sufrido acoso en línea.[5] En México, 33 por ciento de los adolescentes ha sido víctima de ciberbullying, y según el Módulo sobre Ciberacoso (Mociba) del Instituto Nacional de Estadística y Geografía (INEGI), la prevalencia de ciberacoso entre personas de 12 años y más que usan internet fue significativa, con Tlaxcala registrando la mayor incidencia, seguido de Yucatán y Tabasco. Las mujeres jóvenes son particularmente vulnerables, pero el ciberacoso más frecuente que experimentaron ambos sexos fue el contacto mediante *identidades falsas.* [6]

El *ciberbullying* , por su parte, es una de las manifestaciones más comunes de violencia digital, e incluye amenazas, hostigamiento y humillaciones constantes en redes sociales, mensajes de texto y plataformas digitales. Su impacto en niñas, niños y adolescentes es devastador, ya que puede generar ansiedad, depresión e incluso pensamientos suicidas. La UNICEF ha señalado que, en México, 70 por ciento de los jóvenes ha presenciado casos de acoso en línea y 35 por ciento ha sido víctima directa de esta forma de violencia.[7]

A la luz de todas las anteriores consideraciones, la presente iniciativa busca responder a la urgente necesidad de actualizar el Código Penal Federal para enfrentar los desafíos del siglo XXI en materia de criminalidad digital, con el propósito de tipificar la “violencia digital” y la “violencia mediática” y establecer las sanciones de los delitos cibernéticos derivados del uso indebido de tecnologías de la información y la comunicación o sistemas de inteligencia artificial en perjuicio de persona alguna.

Es un hecho indiscutible que la ausencia de una tipificación clara de la "violencia digital" y la "violencia mediática" en el Código Penal Federal limita la capacidad del sistema judicial para sancionar adecuadamente las conductas ilícitas que, a través de medios digitales o tradicionales, atenten contra la integridad, dignidad y derechos de las personas, derivado del uso indebido de las TIC y los sistemas de IA que se refleja en la creación y difusión de *deepfakes* con fines maliciosos, exige una actualización del marco legal para abordar eficazmente las nuevas modalidades de delitos cibernéticos, estableciendo penas y sanciones claras y proporcionales que reflejen la gravedad de los delitos y que actúen con efectos disuasivos, además que permitan la protección de los grupos que son más vulnerables a este tipo de ilícitos como son mujeres, niñas, niños y jóvenes.

Por ello, la regulación eficaz de los delitos cibernéticos es fundamental para garantizar la protección de los derechos, la integridad de las instituciones y la confianza en el uso de la tecnología. Con esta reforma a la legislación penal federal, México podrá avanzar hacia la construcción de un marco normativo más robusto y adecuado a las nuevas realidades tecnológicas, que logre fortalecer la seguridad jurídica ante la realidad digital contemporánea y siente las bases para que nuestro país esté acorde con las recomendaciones hechas por organismos internacionales y ello, permita, a su vez, establecer mecanismos de cooperación interinstitucional para la prevención, investigación y sanción de delitos cibernéticos.

En julio de 2024, instituciones nacionales especializadas advirtieron respecto a la importancia de contar con un marco normativo que proteja los derechos de los ciudadanos frente a los posibles riesgos de la IA, incluyendo la generación de contenido simulado que pueda dañar la reputación y privacidad de las personas.[8]

Y aunque a la fecha de presentación de esta iniciativa no se dispone de cifras exactas sobre la incidencia de delitos relacionados con la generación de contenido simulado mediante el uso de las TIC o los sistemas de IA en México, la creciente preocupación de instituciones nacionales e internacionales indica una tendencia al alza en el uso indebido de estas tecnologías.

Finalmente, aunque vivimos en un mundo plural, abierto y tremendamente interconectado, la tipificación de la violencia digital o la violencia mediática jamás podría equipararse a un mecanismo de censura a la libertad de expresión que hoy gozamos a cabalidad los mexicanos; lo que plantea es que ésta pueda ejercerse a través de la banda ancha e Internet, haciendo uso de las TIC y los sistemas de IA, sin menoscabo de la integridad y seguridad de las personas al legislar sobre sanciones y penas que permitan defender la personalidad jurídica y hasta la dignidad humana, pues si bien en el año 2007 se despenalizaron los delitos de injuria, difamación y calumnia de la legislación nacional, el desarrollo y avance científico, tecnológico y digital hoy imponen nuevos retos legislativos.

Por todo lo anteriormente expuesto, se somete a consideración de los integrantes de esta honorable asamblea la siguiente iniciativa con proyecto de

Decreto que reforma el Título Vigésimo

Del Código Penal Federal

Artículo Único. – Se **reforma** el Título Vigésimo del Código Penal Federal, para quedar como sigue:

Código Penal Federal

Título Vigésimo Delitos cibernéticos

Capítulo I Violencia digital

Artículo 344.- Se clasifica como violencia digital todo acto realizado mediante el uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial, por el que, a través de la banda ancha o Internet, se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos simulados de una persona, sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico o emocional.

Artículo 345.- Se entenderá por uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial, los recursos digitales como software, aplicaciones y programas informáticos que se utilizan para procesar, administrar, crear, modificar, compartir y difundir datos, información, mensajes, imágenes, audios o videos simulados, a través de la banda ancha e Internet.

Artículo 346.- La difusión de publicaciones haciendo el uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial, tales como plataformas digitales, medios de comunicación, redes sociales, correo electrónico o página de Internet que tengan el propósito de dañar o perjudicar la integridad de la persona, en cualquier ámbito de su vida privada o imagen pública, se considerará como violencia digital.

Los delitos previstos en este artículo se sancionarán con una multa de quinientos a mil Unidades de Medida y Actualización vigentes o, en caso de reincidencia, con una pena de uno a tres años de prisión, contemplándose las reglas de mínimos y máximos previstas en el artículo 363 de este Código.

Artículo 347.- En caso de presumir ser víctima de daño psicológico, emocional, la persona tendrá derecho a que la difusión del contenido negativo sea suspendida como medida provisional, sin que medie petición judicial formal.

En este caso, deberá solicitarlo mediante escrito e identificar plenamente al proveedor de servicios en línea a cargo de la administración del sistema informático, sitio o plataforma de Internet en donde se encuentre alojado el contenido y la localización precisa del contenido en Internet, señalando el Localizador Uniforme de Recursos (URL).

El proveedor de servicios en línea en donde se encuentre alojado el contenido presuntamente negativo dará aviso inmediato al usuario que compartió el contenido original, que su difusión y/o transferencia replicada habrá de suspenderse, señalándole de forma clara y precisa los términos de uso y avisos de privacidad que suscribió. En caso contrario, pagarán una multa de quinientas a dos mil Unidades de Medida y Actualización vigente.

Dentro de los cinco días siguientes a la solicitud de la medida provisional de protección prevista, a petición de parte podrá celebrarse una audiencia en la que la persona juzgadora podrá solicitar el resguardo y conservación lícita e idónea del contenido que se denunció de acuerdo con sus características, con el propósito de ratificar o modificarla considerando la información disponible, así como la irreparabilidad del daño.

Capítulo II

Artículo 348.- Se clasifica como violencia mediática todo acto por el que de manera directa o indirecta, haciendo uso de las tecnologías de la información y la comunicación o sistemas de inteligencia artificial, se promuevan a través de cualquier medio de comunicación actos de discriminación que causen daño psicológico, sexual, físico, económico o patrimonial.

Artículo 349.- La violencia mediática se ejerce por cualquier persona física o moral que utilice un medio de comunicación para producir y difundir contenidos modificados mediante el uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial, que atenten contra la autoestima, salud, integridad, libertad y seguridad de las personas.

Artículo 350.- Dentro de la violencia mediática, no es punible la libertad de difundir opiniones, información e ideas, a través de cualquier medio de comunicación, salvo contenido que contenga imágenes, audios o videos simulados de una persona que impliquen casos de ataque a la moral, la vida privada, los derechos de terceros, provoque algún delito o perturbe el orden público.

Artículo 351.- Constituye un acto de violencia mediática, la difusión por cualquier medio de comunicación, de una imagen, audio o video simulado, mediante el uso de las tecnologías de la información y la comunicación o sistemas de inteligencia artificial, que sea falso o alterado y cause daño o perjudique la integridad de la persona, en cualquier ámbito de su vida privada o imagen pública.

Artículo 352.- La persona que, a través de cualquier medio de comunicación, o haciendo uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial ejerza su derecho a la libertad de expresión, respetará el derecho a la intimidad personal y familiar, y a la protección de los datos personales.

Artículo 353.- La acción penal de los capítulos I y II del presente título prescriben en un año, si el delito sólo mereciere multa; si el delito mereciere, además de esta sanción, pena privativa de libertad o alternativa, se atenderá a la prescripción de la acción para perseguir la pena privativa de libertad; lo mismo se observará cuando corresponda imponer alguna otra sanción accesoria.

Artículo 354.- Se perseguirán de oficio los delitos cibernéticos que impliquen casos de ataque a la moral, la vida privada, los derechos de terceros, provoque algún delito o perturbe el orden público.

Artículo 355.- Se sancionará al que haciendo uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial:

I. Genere, altere o difunda contenido digital que contenga imágenes, audio o video reales o simulados, de una persona, sin su consentimiento, aprobación o autorización, con el propósito de suplantar su identidad, dañar su imagen u obtenga lucro o beneficio de ésta, causando daño psicológico emocional.

II. Genere contenido digital, tales como imágenes, audio o video simulados de una persona, de situaciones falsas, o las difunda teniendo conocimiento de su falsedad, con el propósito de desinformar, inducir al error, obtener un lucro o ventaja indebida; salvo que adviertan de manera clara y visible y/o en marca de agua la leyenda: "MEME" entendida como una imagen, audio, video o texto, por lo general imitada o distorsionada con fines caricaturescos, que se difunde a través de la banda ancha y la Internet.

III. Genere, difunda o altere mediante el uso de sistemas de inteligencia artificial, imágenes, audios o videos de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.

A quien cometa los delitos previstos en las fracciones I y II, se le impondrá una multa de quinientas a mil Unidades de Medida y Actualización vigente. En caso de reincidencia, podrá imponerse una pena de uno a tres años de prisión.

A quien cometa los delitos previstos en la fracción III, se le impondrá pena de prisión de tres a seis años, y una multa de quinientas a mil Unidades de Medida y Actualización vigente, así como el decomiso y destrucción de los objetos, instrumentos y productos del delito.

Las penas previstas en los párrafos cuarto y quinto de este artículo se impondrán también a quien posea, almacene, distribuya, financie, venda, compre, arriende, exponga, publicite, enajene, facilite o transmita, el material a que se refiere la fracción III de este artículo.

Las penas previstas para la fracción III, se agravarán en su mínimo y máximo hasta en una mitad cuando la víctima sea menor de edad.

Las mismas penas del párrafo anterior se aplicarán a quien realice las conductas descritas en la fracción III, respecto a persona que no se tenga certeza de su identidad o existencia, pero aparente ser menor de edad, aun cuando el contenido lesivo no corresponda con la persona que es señalada o identificada en los mismos.

Las penas previstas en el presente artículo se agravarán en su mínimo y máximo hasta en dos terceras partes cuando a consecuencia de los efectos o impactos del delito, la víctima atente contra su integridad o contra su propia vida.

Capítulo III Ciberbullying y ciberacoso

Artículo 356.- Se clasifica como delito de ciberbullying cuando una persona sufre maltrato, molestia, discriminación, burla u hostigamiento a través del uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial. Éste se agrava si se comete en contra de una persona especialmente vulnerable por razón de su edad, género o condición social.

Artículo 357.- Se clasifica como delito de ciberacoso la intimidación repetitiva de una persona, que tiene el propósito de amenazar, atemorizar, enfadar o humillarla a través del uso de tecnologías de la información y la comunicación o sistemas de inteligencia artificial, incluyendo la creación de cuentas falsas o bots.

Artículo 358.- Para garantizar los derechos humanos de las personas adolescentes a quienes se les impute o resulten responsables de la comisión de actos tipificados como delitos conforme a este título, se observarán las normas previstas por la Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes, según su grupo etario.

Artículo 359.- En el caso de que estos delitos tengan relación con contenido sexual con personas menores de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen la capacidad para resistirlo, se observarán las disposiciones contempladas en el Título Séptimo Bis de este Código, relativo a los delitos contra la indemnidad de privacidad de la información sexual.

Si se acosa a una persona vulnerable por razón de su edad, género o condición social, se establecerá una pena de prisión de seis meses a dos años, sin derecho a multa.

Capítulo IV Disposiciones comunes para los capítulos precedentes

Artículo 360.- Las medidas de protección, providencias precautorias y medidas cautelares de los delitos de violencia digital, mediática, ciberbullying y ciberacoso observarán las normas previstas por el Código Nacional de Procedimientos Penales.

Artículo 361.-Tratándose de violencia digital o mediática, para garantizar la integridad de la presunta víctima, la o el Ministerio Público o la persona juzgadora ordenarán de manera inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito al proveedor de servicios en línea a cargo de la administración del sistema informático, sitio o plataforma de Internet en donde se encuentre alojado el contenido digital perjudicial para la persona, la interrupción, bloqueo, destrucción o eliminación de imágenes, audios o videos reales o simulados, relacionados con la investigación previa satisfacción de los requisitos de Ley.

Artículo 362.- La autoridad que ordene las medidas de protección contempladas en este capítulo solicitará el resguardo y conservación lícita e idónea del contenido que se denunció, de acuerdo con sus características.

Artículo 363.- Los delitos previstos en el capítulo III del presente título, se sancionarán con una multa de quinientos a mil Unidades de Medida y Actualización vigentes o, en caso de reincidencia, con una pena de uno a tres años de prisión.

El mínimo y el máximo de la pena se aumentará hasta en una mitad:

I.- Cuando se obtenga algún tipo de beneficio no lucrativo;

II.- Cuando se haga con fines lucrativos, o

III.- Cuando a consecuencia de los efectos o impactos del delito, la víctima atente contra su integridad o contra su propia vida.

Transitorio

Único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Notas

1 Cónfer. Convención de Budapest sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001.

2 Consúltese “Recomendación sobre la ética de la inteligencia artificial”, 30 de agosto de 2023, disponible en la liga: https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

3 “El llamado ‘deepfake’ consiste en imágenes o vídeos que se generan por medio de una técnica de inteligencia artificial. Se trata de un ‘aprendizaje automático’ llamado en inglés deep learning (en español: aprendizaje profundo). Tal como señala la Enciclopedia Británica, deepfake se compone de dos términos ingleses: deep, que refiere a la inteligencia artificial, un aprendizaje automático que a su vez se compone de muchos niveles de procesamiento; y fake, que alude a lo falso del material que se obtiene como resultado. Estás imágenes o videos que son originados por esta IA plasman algo que, a simple vista, parece verídico y realista. Sin embargo, el contenido es falso y se basa en personas que existen o existieron, menciona el organismo mundial.” Vid. “¿Qué es un deepfake?” en National Geographic, 15 de noviembre de 2023, disponible en https://www.nationalgeographicla.com/ciencia/2023/11/que-es-un-deepfake

4 UNICEF, “1 de cada 3 jóvenes dice haber sufrido ciberacoso”, 4 de septiembre de 2019, disponible en la liga: https://www.unicef.es/noticia/1-de-cada-3-jovenes-dice-haber-sufrido-ciberacoso

5 INEGI, Módulo sobre Ciberacoso. Mociba-2022. Principales resultados, México, julio de 2023.

6 Cónfer. Rodrigo López Orozco, “Ciberseguridad. Cómo protegerte en internet”, en UNICEF México, disponible en la liga: https://www.unicef.org/mexico/ciberseguridad

7 Comunicado de Prensa: “El INAI impulsa la regulación de la inteligencia artificial en México”, 5 de julio de 2024.

Dado en el salón de sesiones de la Cámara de Diputados, a 5 de marzo de 2025.

Diputado Ricardo Monreal Ávila (rúbrica)