INICIATIVA QUE ADICIONA EL ARTÍCULO 199 OCTIES DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE CREACIÓN DE CONTENIDOS ÍNTIMOS MEDIANTE INTELIGENCIA ARTIFICIAL, A CARGO DE LA DIPUTADA LILIA AGUILAR GIL, DEL GRUPO PARLAMENTARIO DEL PT

La que suscribe, Lilia Aguilar Gil, en mi carácter de diputada federal, integrante del Grupo Parlamentario del Partido del Trabajo de la LXVI Legislatura de la Cámara de Diputados del honorable Congreso de la Unión, con fundamento en lo dispuesto en la fracción II del artículo 71 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 77 y 78 del Reglamento de la Cámara de Diputados, someto a consideración del honorable Congreso de la Unión la presente **iniciativa con proyecto de decreto por el que adiciona un párrafo tercero al artículo 199 Octies del Código Penal Federal**, al tenor de la siguiente.

Exposición de Motivos

La inteligencia artificial representa una oportunidad emprendedora sin precedentes para impulsar la innovación y la transformación digital en los modelos de negocio, convirtiéndose en un pilar fundamental para la competitividad empresarial en la era digital.

Si bien, la inteligencia artificial (IA) se ha convertido en un motor de innovación y desarrollo a nivel global, en México no es la excepción, de acuerdo con el reporte "Estado de Preparación en inteligencia artificial de México", elaborado por la Unesco en colaboración con la Alianza Nacional para la inteligencia artificial (ANIA) y el Centro-i para la Sociedad del Futuro.

El reporte, refiere una visión detallada sobre el estado actual y los desafíos que enfrenta el país en materia de desarrollo e implementación de herramientas e, se realizó mediante un este estudio involucró a más de 250 representantes de diversos sectores, entre gobiernos federales y estatales, órganos autónomos, organizaciones civiles, academia y la iniciativa privada.

La inteligencia artificial sirve para automatizar procesos y simular ciertos rasgos de la inteligencia humana mediante sistemas informáticos. Entre las capacidades de la IA se encuentra el reconocimiento de voz, texto e imágenes, la traducción de idiomas y la generación de textos.[1]

Las *Deepfakes* , acrónimo formado por las palabras en inglés *"fake"* (falso) y *"deep learning",* un subcampo de la inteligencia artificial. Se trata de un video, una imagen o un audio generado para imitar la apariencia y sonido de una persona y estos son generados de modo artificial, y son tan convincentes, tan realistas que, muchas veces, el ojo humano no percibe que está frente a una imagen ficticia.[2]

En la última década, el avance acelerado de la inteligencia artificial (IA) ha permitido el desarrollo de tecnologías que, aunque prometedoras, también representan riesgos significativos.

Estas herramientas están transformando múltiples sectores, desde la medicina hasta la comunicación, ofreciendo soluciones innovadoras y nuevas posibilidades de interacción. Sin embargo, uno de los desarrollos más controvertidos es el de los *"deepfakes",* herramientas de edición digital que emplean algoritmos avanzados, particularmente redes neuronales generativas, para superponer rostros y voces de personas en videos falsificados con un nivel de precisión inquietante.

Esta tecnología tiene aplicaciones positivas en áreas como el entretenimiento, la educación y la creación de contenido artístico. Por ejemplo, los *deepfakes* han sido utilizados para preservar la voz de personas con enfermedades degenerativas o para recrear personajes históricos en documentales interactivos. No obstante, su uso malicioso ha generado alarmantes consecuencias, especialmente para las mujeres, al convertirse en una herramienta para vulnerar derechos fundamentales y amplificar la violencia digital. malicioso ha generado alarmantes consecuencias, especialmente para las mujeres.

Los *deepfakes* con contenido sexual explícito se han convertido en una herramienta de violencia digital. Según datos de organizaciones especializadas en ciberseguridad, más del 90% de los *Deepfakes* publicados en plataformas en línea tienen como objetivo a mujeres, muchas de las cuales desconocen que su imagen ha sido manipulada. Estos videos no solo atentan contra la privacidad, sino que generan graves daños psicológicos, sociales y profesionales a las víctimas.

Es imperativo legislar para prevenir, sancionar y erradicar la creación y difusión de contenido *deepfake* que vulnera los derechos de las mujeres. La falta de regulación específica sobre este fenómeno perpetúa una cultura de violencia digital, normaliza la objetivación de las mujeres y refuerza estereotipos de género dañinos.

Los daños que sufren las víctimas son múltiples: desde la pérdida de oportunidades laborales hasta el deterioro de su salud mental. Muchas enfrentan el estigma social, la revictimización y la falta de apoyo legal o psicológico. Además, la ausencia de mecanismos efectivos para retirar este contenido de internet agrava su sufrimiento.

Un marco normativo claro no solo protegerá a las víctimas, sino que también enviará un mensaje contundente contra la violencia de género en el entorno digital. La sociedad actual exige que los derechos humanos se extiendan a todos los espacios, incluyendo el virtual.

La violencia digital mediante el uso de *Deepfakes* es una problemática creciente que exige una respuesta contundente y urgente. La presente iniciativa no solo busca reparar un vacío legal, sino garantizar que las mujeres puedan ejercer plenamente sus derechos en un entorno digital seguro y libre de violencia. Proteger la dignidad, privacidad y seguridad de las mujeres no es solo un acto de justicia, sino un paso indispensable hacia una sociedad más igualitaria y respetuosa.

Deepfakes **en el contexto internacional**

A nivel global, el fenómeno de los *deepfakes* plantea desafíos legales, éticos y técnicos que han generado respuestas diversas entre los países. En naciones como Estados Unidos, algunos estados han comenzado a promulgar leyes específicas que penalizan la creación y

difusión de *deepfakes,* especialmente aquellos con contenido sexual explícito o diseñados para interferir en procesos electorales. Sin embargo, estas legislaciones son recientes y todavía presentan vacíos en su alcance y aplicación.

En la Unión Europea, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) ofrece cierta protección al permitir que las víctimas soliciten la eliminación de contenido no autorizado. No obstante, la falta de una legislación específica para los *deepfakes* dificulta abordar el problema de manera integral. Además, iniciativas como la Ley de Servicios Digitales buscan establecer obligaciones más claras para las plataformas en línea respecto a la detección y eliminación de contenido dañino.

Por otro lado, países como China han adoptado un enfoque regulatorio más restrictivo, exigiendo que los contenidos generados mediante IA incluyan marcas de agua digitales para identificar su naturaleza artificial. Aunque estas medidas son un avance, su efectividad depende en gran medida de la implementación y de la cooperación internacional.

La cooperación internacional resulta esencial, dado que los *Deepfakes* , al ser distribuidos principalmente en plataformas globales, trascienden fronteras. Organismos como la Interpol han señalado la necesidad de establecer marcos colaborativos que permitan rastrear y sancionar a los responsables de este tipo de violencia digital. Sin embargo, las diferencias culturales, legales y tecnológicas entre los países dificultan la creación de un consenso global.

Es crucial que las naciones trabajen juntas para desarrollar estándares internacionales que regulen el uso de tecnologías como los *Deepfakes* , garantizando que estas herramientas no se utilicen para vulnerar derechos fundamentales. Además, se requiere de un diálogo constante entre gobiernos, empresas tecnológicas y organizaciones de la sociedad civil para abordar los desafíos técnicos y éticos que plantean los *Deepfakes* .

Vigilancia y seguimiento

Ha nivel internacional existe un estudio realizado por “Security Hero.io” en el que han llevado a cabo una investigación del impacto de las “*Deepfakes* ” en los cuales han reportado hallazgos del alcance de las mismas.[3]

Según el estudio reporta que:

• La pornografía *deepfake* constituye el 98 por ciento de todos los vídeos *deepfake* en línea.

Lo que constituye que la mayoría de la distribución de *Deepfakes* están relacionadas con la creación de video de contenido sexual, con distintas intenciones como difamar, violentar y denigrar.

• Hay un 550 por ciento más de vídeos *deepfake* en línea en 2023 que en 2019.

En solo un par de años la cantidad de videos tienden a la alza lo que preocupa su aceptación y normalización en el ámbito secular.

• 7 de los 10 principales sitios web de pornografía albergan *Deepfakes*

Su consumo se ha vuelto accesible, su distribución no representa un reto siendo que los propios sitios web contienen estos videos, lo que además de ser fácil de visualizar y/o compartir, representa la normalización de este tipo de contenido, lo que incita a replicar dicho contenido dirigido a personas de su interés personal.

• Entre 2022 y 2023, la cantidad de pornografía *deepfake* creada aumentó un 464 por ciento

Esto representa una clara tendencia y crecimiento exponencial de su uso enfocado a la generación de contenido sexual.

• El 99 por ciento de las personas afectadas por pornografía *deepfake,* son mujeres.

Esto evidencia una alarmante disparidad de género en este tipo de agresiones. Este dato es revelador no solo por el alcance del problema, sino porque pone de manifiesto una dinámica de poder subyacente en la violencia digital. Las mujeres, debido a su alta exposición mediática o simplemente por su presencia en plataformas digitales, son constantemente objeto de manipulación y explotación mediante esta tecnología, lo cual perpetúa estereotipos de género y las revictimiza en un entorno que debería ser seguro y respetuoso.

• Disponibilidad de herramientas, software y comunidades fáciles de usar para crear *Deepfakes* .

El crecimiento exponencial de los *Deepfakes* ha sido facilitado en gran medida por la disponibilidad de herramientas y software accesibles al público general. Existen múltiples aplicaciones, muchas de ellas de uso gratuito o a bajo costo, que permiten a cualquier persona con conocimientos básicos de informática crear contenido manipulado. Plataformas como GitHub, foros en línea y comunidades específicas en redes sociales han contribuido a la rápida difusión de estas tecnologías, proporcionando tutoriales, algoritmos preentrenados y recursos para generar *Deepfakes* con relativa facilidad.

Esta accesibilidad tecnológica plantea un grave problema, ya que permite que personas sin formación técnica puedan producir videos manipulados con fines maliciosos. Las comunidades en línea que promueven el uso de *Deepfakes* a menudo normalizan su creación y consumo, minimizando el impacto ético y legal de estas acciones. Estas redes también facilitan la distribución masiva de contenido manipulado, lo que aumenta la exposición y revictimización de las personas afectadas.

Es importante destacar que esta disponibilidad de herramientas no solo fomenta el uso malintencionado, sino que también dificulta la regulación efectiva del fenómeno. La velocidad a la que evolucionan las tecnologías de *Deepfake* supera con creces el ritmo de las respuestas legislativas y técnicas, dejando a las víctimas en una situación de vulnerabilidad constante.

Abordar este problema requiere no solo una regulación más estricta, sino también una mayor colaboración entre las plataformas tecnológicas, las autoridades gubernamentales y las organizaciones de la sociedad civil.

En México, la creciente era digital ha aumentado la productividad y eficiencia, mejorado la comunicación y fomentado la innovación. Pero a su vez, también ha traído consigo el surgimiento de nuevas y sofisticadas formas de reproducción de otros tipos de violencia. Históricamente, esta violencia no ha afectado a todas las personas de la misma manera.

Uno de los aspectos más inquietantes de los *Deepfakes* es su conexión con la venganza mediante la diseminación de contenido íntimo y sexualmente explícito. Esto ocurre cuando, sin el consentimiento de una persona, su pareja, expareja o terceros difunden o amenazan con difundir imágenes intimas sexualmente explicitas de ella, con el propósito de controlarla, castigarla y/o dañar su reputación. Algunas investigaciones han documentado los patrones de género sobre este fenómeno, mostrando que esta afecta desproporcionadamente a mujeres en comparación con los hombres, lo que la convierte en otra forma de violencia de género.[4]

Las víctimas de *Deepfakes* pueden llegar a presentar ansiedad generalizada, a la vez que intentan lidiar con la vergüenza, el enojo, la humillación y el estigma. La violación de su privacidad y la difusión de imágenes manipuladas pueden afectar profundamente su salud mental, y por ende su calidad de vida, e incluso causarles trauma. Además, puede tener repercusiones en las relaciones personales y las oportunidades profesionales de las mujeres afectadas.

Es necesario fomentar la investigación y el desarrollo de herramientas de detección que puedan identificar y bloquear contenido manipulado antes de su difusión masiva.

Por lo anterior, con este tipo de iniciativas se procura hacer más accesible la denuncia de esta y otras formas de agresión en el ámbito digital, lo cual permite la sanción efectiva de las personas responsables.

A efecto de lograr una mejor comprensión de la propuesta se inserta el siguiente cuadro comparativo.

CÓDIGO PENAL FEDERAL	
Texto Vigente	**Texto propuesto**
Artículo 199 Octies.- Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.	...
Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.	...
SIN CORRELATIVO	**Así mismo, la utilización de técnicas, aplicaciones o programas de inteligencia artificial para la creación, manipulación y distribución de videos, audios, imágenes e impresiones con contenido intimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.**
Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.	....
TRANSITORIOS	
	Único. El presente Decreto entrará en vigor el día después al de su publicación en el Diario Oficial de la Federación.

Por lo anteriormente expuesto, acudo a esta soberanía a presentar, iniciativa con proyecto de:

Decreto por el que se adiciona un párrafo tercero al artículo 199 Octies y se recorre el subsecuente, del Código Penal Federal

Único. Se adiciona un párrafo tercero al artículo 199 Octies y se recorre el subsecuente, del Código Penal Federal, para quedar como sigue:

Artículo 199 Octies. ...

...

Asimismo, la utilización de técnicas, aplicaciones o programas de inteligencia artificial para la creación, manipulación y distribución de videos, audios, imágenes e impresiones con contenido intimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.

...

Transitorio

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

Notas

1 https://www.eleconomista.com.mx/tecnologia/Mexico-esta-preparado-para-l a-Inteligencia-Artificial-20240704-0049.html

2 Infografía IPN https://www.seguridad.ipn.mx/comunicados/Infografia_Deepfake.pdf

3 Security Hero.io https://www.securityhero.io/state-of-deepfakes/#overview-of-current-stae

4 https://blogs.iadb.org/igualdad/es/deepfakes-violencia-basada-en-genero -inteligencia-artificial/

Palacio Legislativo de San Lázaro a 10 de diciembre de 2025.

Diputada Lilia Aguilar Gil (rúbrica)