INICIATIVA QUE ADICIONA DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE ROBO DE IDENTIDAD, SUSCRITA POR EL DIPUTADO ALAN SAHIR MÁRQUEZ BECERRA Y LAS Y LOS LEGISLADORES INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PAN

El que suscribe, Alan Sahir Márquez Becerra, integrante del Grupo Parlamentario del Partido Acción Nacional en la LXVI Legislatura de la Cámara de Diputados, con fundamento en los artículos 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos; y 6, numeral 1, fracción I, 77, 78 y demás relativos del Reglamento de la Cámara de Diputados, somete a consideración del pleno de esta asamblea iniciativa con proyecto de decreto por el que se adicionan la fracción XVII al artículo 11 Bis y el capítulo I Bis, "Robo de identidad", con los artículos 381 Quinquies y 381 Sexties, al Código Penal Federal, al tenor de la siguiente

Exposición de Motivos

En la actualidad, el desarrollo de la inteligencia artificial (IA), permite la generación de imágenes y videos hiperrealistas sin precedentes, con un alto nivel de precisión de las imágenes o videos; estas innovaciones tecnológicas tienen aplicaciones positivas en la vida diaria de las personas, en actividades como el entretenimiento, la educación y el marketing. Sin embargo, esta tecnología también es utilizada de manera indebida, ya sea para fines ilícitos o para la creación de contenido que vulnera los derechos de identidad de las personas, incluyendo la generación y manipulación de imágenes sin consentimiento, robo de identidad y la difusión de desinformación, así como el derecho a la privacidad, generando violaciones a la propiedad intelectual.

En materia internacional se encuentra el Convenio de Budapest elaborado en 2001 por el Consejo de Europa, que tiene como fin combatir los delitos informáticos, el cual establece la tipificación de delitos en materia de confidencialidad, integridad, datos informáticos, así como la ciberdelincuencia y la importancia de la coordinación y cooperación internacional en materia penal, el cual puede constituir un modelo a seguir en la materia. Sin embargo, México no es parte del convenio, aunque solicitó su adhesión en 2006, por lo que es el único tratado internacional vinculante en la materia. El capítulo II, *Medidas que deberán adoptarse a nivel internacional,* del convenio establece cuatro categorías de delitos:

1. Contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos (acceso ilícito, intercepción ilícita, ataques a la integridad de los datos o del sistema, abuso de los dispositivos).

2. Informáticos (falsificación y fraude informático).

3. Relacionados con el contenido (pornografía infantil).

4. Relacionados con infracciones a la propiedad intelectual.

En el mismo sentido, de acuerdo con la Agenda 2030 de la Organización de las Naciones Unidas (ONU), el Objetivo de Desarrollo Sostenible, en su meta 17.8 busca implementar

mecanismos de apoyo en materia de ciencia, tecnología e innovación para los países menos adelantados y aumentar la utilización de tecnologías instrumentales, en particular la tecnología de la información y las comunicaciones. Por ello, la cooperación y el intercambio de conocimientos entre países resulta fundamental para promover mecanismos que deriven en la reducción de ataques a los derechos de identidad a través de la inteligencia artificial.

Sumado a los anterior, la Organización para la Cooperación y el Desarrollo Económicos desarrolló recomendaciones sobre la inteligencia artificial, en el punto *1.4. Solidez, seguridad y protección* menciona, que los sistemas de IA deben ser seguros, robustos y estar protegidos ante cualquier riesgo; y que deben existir mecanismos cuando la IA provoque daños indebidos o muestren un comportamiento indeseado, estos puedan ser invalidados, corregidos y/o desmantelados de forma segura, según sea necesario; garantizando la integridad de la información.

La International Business Machines lanzó el X-Force Threat Intelligence Index 2024, un informe que analiza las tendencias de ciberamenazas, con el objetivo de ayudar a las empresas a tomar medidas de seguridad proactivas, resaltando en su informe una crisis emergente respecto a las identidades robadas por ciberdelincuentes, hacia empresas en todo el mundo. Sin embargo los ataques no se llevan a cabo solo a empresas, sino también a particulares. El informe menciona que hubo un incremento de 71 por ciento en los ciberataques causados por la explotación de la identidad a nivel mundial.

En 2017 se presentó la Estrategia Nacional de Ciberseguridad con el objetivo de identificar y establecer acciones de seguridad cibernética aplicables a las áreas social, económica y política para permitir a la población y las organizaciones públicas y privadas el uso de las tecnologías de información, de manera responsable para el desarrollo sostenible del Estado mexicano, sin embargo, no hay una actualización y aún existen lagunas jurídicas y retos por atender en la materia.

La Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares de 2020, publicada por el Inegi y la Secretaría de Infraestructura, Comunicaciones y Transportes, menciona que en el país hay 84.1 millones de usuarios de internet (72.0 por ciento de la población de 6 años o más), y 88.2 millones de usuarios de teléfonos celulares (75.5 por ciento de la población de 6 años o más). Comprueba que la mayoría de la población podría enfrentar un riesgo de robo de información.

De igual manera, 9 de cada 10 usuarios de teléfono celular disponen de un celular inteligente *(smartphone).* Entre 2019 y 2020, los usuarios que sólo dispusieron de celular inteligente registraron un crecimiento de 3.5 puntos porcentuales (88.1 a 91.6 por ciento). La encuesta estima que, en 2020, de los usuarios que se conectaron a internet mediante su celular inteligente (Smartphone), se observó un aumento de quienes se conectaron sólo por wifi, que pasaron de 9.4 por ciento en 2019 a 13.7 en 2020. Por lo anterior, las encuestas muestran que cualquier individuo puede experimentar vulneraciones cibernéticas como el robo de identidad.

El Estado mexicano carece de una ley en materia de ciberseguridad, por lo que es urgente disminuir riesgos que vulneren la identidad e información de los mexicanos, mediante las TIC. La ausencia de un marco normativo, que establezca como delito la generación y divulgación de imágenes y videos, sin el consentimiento del propietario, pone en peligro la seguridad de los datos personales y la protección de los derechos fundamentales de las personas.

También el derecho a la protección de datos personales se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos, establecido en el artículo 6o., inciso A, fracción II, que a la letra menciona:

> **A).** ...
>
> ...
>
> La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Para tal efecto, los sujetos obligados contarán con las facultades suficientes para su atención.
>
> Además, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A, y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, establece las bases, principios y procedimientos, en materia de protección y datos personales en posesión de sujetos obligados, tanto físicos como electrónicos.
>
> Aunado a lo anterior, con la reforma publicada en junio de 2014, al artículo 4° constitucional, en su párrafo decimo, se establece que *Toda persona tiene derecho a la identidad* [...], por lo que es un derecho humano universal, reconocido en diversos instrumentos internacionales y en la Carta Magna.
>
> La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) define *robo de identidad:* "cuando una persona obtiene, transfiere, utiliza o se apropia de manera indebida, de los datos personales de otra sin la autorización de esta última, usualmente para cometer un fraude o un delito".

Con datos de la Condusef, se atendieron 802 reclamaciones por posible robo de identidad en los primeros cuatro meses de 2021. A abril, las acciones de defensa para atender un posible robo de identidad ascendieron a mil 410, de las cuales 608 fueron asesorías y 802 se concretaron como reclamaciones (57 por ciento del total). En los primeros cuatro meses de 2021, las reclamaciones por un posible robo de identidad mostraron una reducción de 33.4 por ciento respecto a igual periodo de 2020.

ACCIONES DE DEFENSA PROTOCOLO PORI (Posible Robo de Identidad)
ENERO - ABRIL 2020-2021

PROCESO	2020	2021		
		Núm.	Part.(%)	Var.(%)
TOTAL	2,000	1,410	100.0	-29.5
ASESORIAS*	796	608	43.1	-23.6
RECLAMACIONES	1,204	802	56.9	-33.4

*No incluye 217 asesorías por emisión y 154 por bloqueo de RCE en 2020, y 108 y 139 en 2021 respectivamente, en virtud de que las realizan las Sociedades de Información Crediticia.

Fuente: Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, CONDUSEF, 2021.

Ante ello la Condusef emitió algunas recomendaciones como el no proporcionar información de las cuentas bancarias, cambiar contraseñas con frecuencia y en caso de robo de identificaciones, acudir al Ministerio Público, entre otras. Si bien estos elementos son de relevancia, la tecnología sigue in crescendo, por lo que las recomendaciones se tienen que actualizar con cierta periodicidad.

Existen diversas modalidades de robo de datos personales denominados como fraudes cibernéticos, como el *smishing* **,** que es el envío de un mensaje de texto al teléfono móvil, a finde visitar un página web fraudulenta para obtener tu información personal; igualmente se encuentra el *phishing* , también conocido como suplantación de identidad en materia financiera de tu cuenta bancaria para hacerse pasar por institución financiera y obtener información confidencial como contraseñas, números de tarjetas, claves, etcétera. También existe el *vishing,* donde los ciberdelincuentes simulan ser empleados de una institución bancaria, solicitando información personal para el robo de esta. Igualmente se encuentra el *pharming,* que consiste en redirigirte a una página de internet falsa mediante ventanas emergentes para el robo de información.

Si bien el Estado mexicano cuenta con algunos ordenamientos jurídicos para hacer frente a ataques y amenazas a través de las TIC, así como instrumentos vinculantes para el Estado, en los que se regulan algunos elementos; el robo de identidad o también llamada suplantación de identidad, no se encuentra tipificado como delito.

Derivado de lo anterior, la finalidad de la presente iniciativa es tipificar el robo de identidad, ya que este delito en el pasado, solo se limitaba a la falsificación de documentos, sin embargo con el avance tecnológico, se comete a través de la IA. La inteligencia artificial ha revolucionado diversos aspectos de la vida actual, nos ha permitido mejorar la comunicación, el acceso a la información y la automatización de tareas en varios sectores. Sin embargo, también ha abierto la puerta a nuevas formas de fraude y manipulación digital. Hoy, mediante algoritmos avanzados, es posible crear imágenes, videos y audios que replican con precisión la voz y el rostro de una persona, sin su conocimiento, ni consentimiento. Esto pone en riesgo no solo la reputación de los ciudadanos, sino su integridad financiera y su seguridad personal.

Por lo anterior, regular el uso de inteligencia artificial en la generación de imágenes y videos con el fin de prevenir la creación y difusión de contenido, que trasgreda los derechos de los

propietarios de la imagen o video de su identidad, garantizaría el respeto a la privacidad, la identidad y la integridad de las personas.

El avance tecnológico debe ir acompañado de normativas que protejan los derechos individuales y colectivos. Esta iniciativa busca equilibrar la innovación con la responsabilidad social, asegurando que el uso de la inteligencia artificial de manera indebida sea penado, por lo que generaría menor incidencia en el uso no autorizado de IA, en la generación de contenido digital, estableciendo sanciones para quienes infrinjan los derechos de terceros. Por lo que es necesario:

- Actualizar el Código Penal para tipificar el uso de IA en el robo de identidad como un delito grave.

- Implantar sanciones para quienes manipulen contenido digital con fines ilícitos.

- Establecer la obligación para las plataformas digitales, a identificar y eliminar contenido generado por IA que viole los derechos de las personas.

La tecnología debe ser una herramienta de progreso y no un instrumento de vulneración de derechos.

El cuadro que a continuación se presenta sintetiza en qué consiste la adición de la fracción XVII del artículo 11 Bis; y el capítulo I Bis, “Robo de identidad”, con los artículos 381 Quinquies y 381 Sexties, al Código Penal Federal, propuesta:

CÓDIGO PENAL FEDERAL	
Texto vigente	**Texto Propuesto**
Artículo 11 Bis.- Para los efectos de lo previsto en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, a las personas jurídicas podrán imponérseles algunas o varias de las consecuencias jurídicas cuando hayan intervenido en la comisión de los siguientes delitos: **A.** De los previstos en el presente Código: **I.** ... a **XVI.** ... **B. ...** **I. ... a XXII. ...** ... **a) ... a e) ...** **...** **[sin correlativo]**	**Artículo 11 Bis.-** ... **A.** ... **I.** ... a **XVI.** ... **B. ...** **I. ... a XXII. ...** **...** **a) ... a e) ...** **...** **XVII. Robo de identidad, previsto en los artículos 381 Quinquies y 381 Sexies;**
[sin correlativo]	**CAPITULO I BIS** **Robo de Identidad** **Artículo 381 Quinquies. - Comete el delito de robo de identidad: la persona que, por cualquier medio, a través de la inteligencia artificial, o tecnologías de la información, obtenga, posea, utilice, transfiera, reproduzca o manipule datos personales, imágenes, videos, audios o cualquier otro elemento identificativo de una persona sin su consentimiento, con el propósito de suplantar su identidad, para obtener**

	un beneficio indebido o causar un daño. Artículo 381 Sexies. - Se sancionará con pena de 4 a 10 años de prisión y hasta mil días de multa a quien cometa el delito de robo de identidad en términos del artículo anterior. La pena se aumentará en una mitad de lo previsto en el párrafo anterior cuando se utilice la identidad robada para cometer fraudes, generar desinformación o desprestigio, mediante la clonación digital del aspecto físico o la voz; Las sanciones pecuniarias previstas en el presente artículo se aplicarán sin perjuicio de la reparación del daño, cuya multa será de 400 a 600 veces el valor diario de la Unidad de Medida y Actualización, y la eliminación del contenido suplantado de manera inmediata.

Por lo expuesto someto a consideración de esta soberanía el siguiente proyecto de

Decreto por el que se adicionan la fracción XVII al artículo 11 Bis y el capítulo I Bis, "Robo de identidad", con los artículos 381 Quinquies y 381 Sexties, al Código Penal Federal, en materia de robo de identidad

Único. Se **adicionan** la fracción XVII al artículo 11 Bis y el capítulo I Bis, "Robo de identidad", con los artículos 381 Quinquies y 381 Sexties, al Código Penal Federal, para quedar como sigue:

Artículo 11 Bis. ...

A. ...

I. a **XVI.** ...

B. ...

I. a **XXII.** ...

...

a) a **e)** ...

...

XVII. Robo de identidad, previsto en los artículos 381 Quinquies y 381 Sexties;

Capítulo I Bis
Robo de Identidad

Artículo 381 Quinquies. - Comete el delito de robo de identidad: la persona que, por cualquier medio, a través de la inteligencia artificial, o tecnologías de la información, obtenga, posea, utilice, transfiera, reproduzca o manipule datos personales, imágenes, videos, audios o cualquier otro elemento identificativo de una persona sin su consentimiento, con el propósito de suplantar su identidad, para obtener un beneficio indebido o causar un daño.

Artículo 381 Sexties. Se sancionará con pena de 4 a 10 años de prisión y hasta mil días de multa a quien cometa el delito de robo de identidad en términos del artículo anterior.

La pena se aumentará en una mitad de lo previsto en el párrafo anterior cuando se utilice la identidad robada para cometer fraudes, generar desinformación o desprestigio, mediante la clonación digital del aspecto físico o la voz;

Las sanciones pecuniarias previstas en el presente artículo se aplicarán sin perjuicio de la reparación del daño, cuya multa será de 400 a 600 veces el valor diario de la Unidad de Medida y Actualización, y la eliminación del contenido suplantado de manera inmediata.

Transitorios

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

Segundo. Las plataformas digitales y redes sociales contarán con un plazo de 90 días naturales, a partir de la entrada en vigor del presente Decreto, para establecer mecanismos

que permitan la detección y eliminación de contenido que vulnere la identidad de las personas conforme a lo establecido en este.

Palacio Legislativo de San Lázaro, a 9 de septiembre de 2025.

Diputado Alan Sahir Márquez Becerra (rúbrica)