

INICIATIVA QUE ADICIONA EL TÍTULO VIGÉSIMO SÉPTIMO AL LIBRO SEGUNDO Y EL ARTÍCULO 430 AL CÓDIGO PENAL FEDERAL, A CARGO DE LA DIPUTADA CLAUDIA ALEJANDRA HERNÁNDEZ SÁENZ, DEL GRUPO PARLAMENTARIO DE MORENA.

La que suscribe, diputada Claudia Alejandra Hernández Sáenz, en la LXVI Legislatura del Congreso de la Unión, integrante del Grupo Parlamentario de Morena, con fundamento en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos y en los artículos 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente iniciativa con proyecto de decreto que adiciona el título vigésimo séptimo al libro segundo y el artículo 430 al Código Penal Federal, en materia de usurpación de identidad, al tenor de la siguiente

Exposición de Motivos

La suplantación de identidad ha existido desde las civilizaciones antiguas, manifestándose como falsificación de actas, suplantación de nombres en herencias o el uso de documentos apócrifos. En ese entonces, el delito tenía un alcance limitado, ya que dependía de interacciones físicas y del manejo de documentación impresa.

En el siglo XX se consolidó la identidad legal y adquirió un carácter estructural dentro de los sistemas burocráticos. Documentos como pasaportes, cédulas fiscales y números de seguridad social, se convirtieron en llaves de acceso a servicios, lo que generó a su vez una proliferación en las técnicas de falsificación y suplantación.¹

Con la llegada del internet en los años noventa, se produjo un cambio radical. La identidad dejó de ser únicamente física para convertirse en un conjunto de datos digitales — contraseñas, correos electrónicos, tokens, imágenes—, lo que facilitó su robo y explotación remota. Esta etapa dio paso a fenómenos masivos como el phishing, spoofing, y los fraudes por correos electrónicos no solicitados (spam).²

Diversos estudios y organismos especializados en ciberseguridad han documentado que los correos electrónicos fraudulentos, a pesar de ser los métodos más comunes de suplantación de identidad, no suelen solicitar de forma inmediata información sensible; sino que emplean técnicas de ingeniería social para construir una narrativa persuasiva que inspire confianza.³ Es frecuente que los ciberdelincuentes se hagan pasar por ejecutivos bancarios, abogados o representantes de organismos internacionales, utilizando logotipos de empresas como Microsoft, PayPal o instituciones financieras.

Cabe destacar que los delincuentes priorizan la obtención de datos básicos como correos electrónicos, teléfonos y nombres para establecer el primer contacto. Este patrón confirma que el eje central del delito de usurpación digital radica en la manipulación emocional de la víctima.

Sin embargo, la usurpación de identidad, especialmente en su dimensión digital, ha evolucionado en escala, sofisticación y complejidad psicológica. Hoy, los ataques se basan más en la construcción de confianza que en la vulneración técnica directa.⁴ Por tanto, la

solución no es solamente tecnológica, sino cultural y legal, promoviendo una ciudadanía digital crítica y una legislación adaptativa.

En este sentido, la era digital marca el punto de inflexión en la historia de la suplantación de identidad. A partir de los años noventa, la digitalización de servicios públicos y financieros multiplicó exponencialmente el riesgo de exposición de datos personales: direcciones de correo electrónico, contraseñas, números de tarjetas, fotografías y documentos escaneados.

Es decir, el delito dejó de requerir contacto físico con documentos, volviéndose una operación remota, automatizada y masiva.

Uno de los hitos más importantes en esta evolución fue la aparición del phishing y el malware, técnicas utilizadas para engañar a los usuarios y robar sus credenciales digitales. A esto se suman los grandes robos de bases de datos, como el de Equifax en 2017, que expuso la información personal de más de 147 millones de personas en Estados Unidos.⁵

En los últimos años, la irrupción de la inteligencia artificial ha planteado nuevos y complejos desafíos para la protección de la identidad. Tecnologías como los deepfakes —videos manipulados con técnicas de aprendizaje profundo que imitan rostros y voces— han llevado la suplantación de identidad a niveles antes inimaginables. Hoy, no solo se roba una identidad legal o financiera, sino también la imagen, la voz y el comportamiento de una persona.

Investigaciones recientes advierten que la inteligencia artificial generativa facilita fraudes más convincentes y personalizados, dificultando su detección por parte de las víctimas y los sistemas de defensa.⁶

A nivel global, la usurpación de identidad se ha consolidado como una de las principales amenazas cibernéticas. Según el Centro de Estudios Estratégicos e Internacionales (CSIS), los delitos relacionados con la identidad generan pérdidas por más de 600 mil millones de dólares anuales, es decir, el 0,8% del PIB mundial.⁷ En América Latina, la carencia de regulaciones robustas y la debilidad de la infraestructura digital agravan esta situación, afectando tanto a personas como a instituciones.

De acuerdo con el Banco de México, el país ocupa el octavo lugar mundial en robo de identidad. Las principales causas incluyen la pérdida de documentos (67 por ciento), el robo de cartera (63 por ciento) y el uso indebido de tarjetas bancarias (53 por ciento).⁸ En 2021, se registraron 49,871 reclamaciones por este delito, lo que representó un aumento del 54 por ciento respecto al año anterior.

Las modalidades actuales son diversas: phishing, vishing (fraude telefónico), smishing (mensajes SMS fraudulentos), skimming (clonado de tarjetas), spyware y ataques tipo man-in-the-middle, que interceptan comunicaciones para robar datos en tiempo real.⁹

En este contexto, la usurpación de identidad debe entenderse como una conducta ilícita de presencia transversal en la sociedad. Se trata de una acción dolosa y antijurídica en la que

una persona utiliza, sin autorización, los datos personales de otra para cometer diversos delitos, manipulando información sensible mediante el engaño y utilizando tanto medios convencionales como Tecnologías de la Información y la Comunicación.¹⁰

La creciente adopción de inteligencia artificial (IA) en procesos financieros, operativos y de comunicación ha facilitado tanto la automatización de servicios como el surgimiento de nuevas modalidades de suplantación de identidad. Según la Compañía para Depósito Central de Valores, S.A. de C.V. (Cecoban) —única empresa autorizada por el Banco de México para operar la Cámara de Compensación Electrónica Nacional, encargada de procesar cheques, transferencias de abono (TEF), transferencias de cargo (domiciliaciones) y compensación de efectivo— los fraudes derivados del robo de identidad pueden generar un daño patrimonial promedio de entre mil y 50 mil pesos por transacción.

Cecoban ha advertido que los avances en IA, particularmente en el procesamiento de imágenes, video y audio, permiten hoy generar contenidos falsos mediante tecnología deepfake, lo cual incrementa el riesgo de creación de identidades artificiales, permanencia digital de personas fallecidas, y fraude mediante suplantación automatizada. Estas capacidades están siendo explotadas por grupos de ciberdelincuencia organizada para alterar solicitudes de crédito y suplantar a usuarios reales, lo que representa un riesgo del 10 por ciento de fraude en nuevas solicitudes, con pérdidas potenciales de hasta 4.5 millones de dólares para las instituciones afectadas.

Asimismo, esta amenaza no impacta de forma homogénea a la población. Un análisis de la consultora The Competitive Intelligence Unit reveló que el 42.4 por ciento de los jóvenes menores de 21 años desconoce los riesgos potenciales de la IA en materia de suplantación de identidad, mientras que entre los adultos mayores de 50 años, solo el 21.9 por ciento desconoce dichos riesgos. Esta disparidad generacional subraya la necesidad de una estrategia integral de educación digital y campañas de concientización, particularmente dirigida a los sectores más jóvenes.

Por su parte, el Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México ha documentado que México ocupa el octavo lugar a nivel mundial en robo de identidad, y que entre 2013 y 2024 la usurpación de identidad mediante IA se incrementó en un 218 por ciento, lo cual reafirma la urgencia de legislar al respecto.¹¹

Pese a la gravedad de esta amenaza, el marco penal federal en México sigue siendo insuficiente. la usurpación de identidad no se encuentra tipificada como delito en el Código Penal Federal, limitando su persecución a figuras genéricas como el fraude.

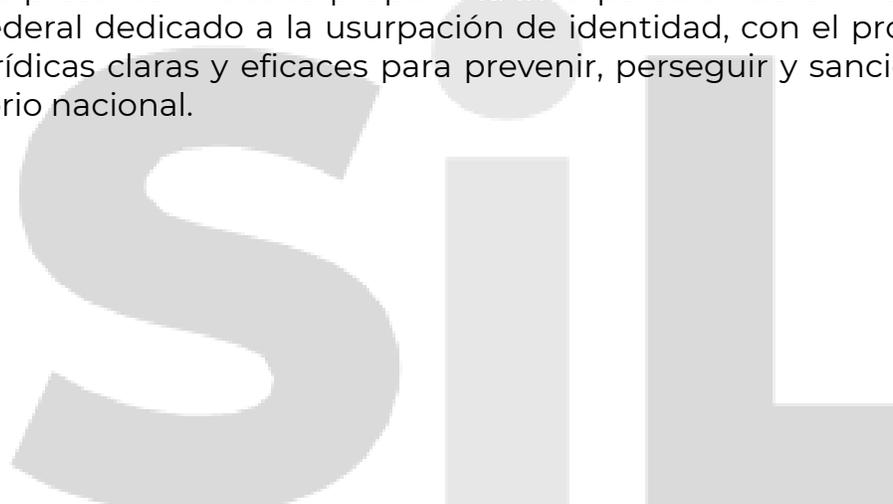
En el ámbito del derecho penal mexicano, la mayoría de las entidades federativas ya han legislado de manera específica sobre el delito de usurpación de identidad, reconociendo su gravedad y creciente impacto en la vida patrimonial, moral y jurídica de las personas. A través de un análisis de derecho comparado,¹² se ha identificado que al menos 27 de las 32 entidades federativas cuentan con disposiciones que tipifican la usurpación o suplantación de identidad, muchas de ellas incluyendo medios electrónicos, digitales o informáticos

entre los mecanismos para su comisión, así como sanciones diferenciadas dependiendo del daño causado o del uso consentido de la identidad ajena.

Este panorama normativo evidencia una preocupación generalizada a nivel estatal por atender el fenómeno de la usurpación de identidad, que se ha intensificado a partir de la digitalización de los servicios financieros, gubernamentales y sociales. En contraste, a nivel federal, aún no se cuenta con una tipificación autónoma y robusta del delito, lo que genera un vacío legal que impide la aplicación uniforme de criterios jurídicos y limita la capacidad de las autoridades federales para investigar y sancionar estas conductas de manera efectiva.

Este desfase entre los avances estatales y la ausencia de regulación a nivel nacional justifica la urgencia de armonizar el marco jurídico federal, a fin de dotar al sistema penal mexicano de herramientas adecuadas para prevenir, perseguir y sancionar la usurpación de identidad en todas sus modalidades, en concordancia con las nuevas dinámicas digitales y los principios de seguridad jurídica y protección de datos personales.

Por lo anterior, la presente iniciativa propone la incorporación de un Título específico en el Código Penal Federal dedicado a la usurpación de identidad, con el propósito de dotar de herramientas jurídicas claras y eficaces para prevenir, perseguir y sancionar esta conducta en todo el territorio nacional.



Ley Federal Penal (Vigente)	Ley Federal Penal (Propuesta)
SIN CORRELATIVO	<p data-bbox="505 243 946 380" style="text-align: center;">TÍTULO VIGÉSIMO SÉPTIMO DELITOS CONTRA LA IDENTIDAD DE LAS PERSONAS CAPITULO ÚNICO USURPACIÓN DE IDENTIDAD</p> <p data-bbox="500 411 954 810">Artículo 430.- Comete el delito de usurpación de identidad la persona que, por cualquier medio, incluyendo el uso de nuevas tecnologías digitales, se atribuya, suplante, apropie o utilice la identidad de otra persona, con la finalidad de acceder a recursos, obtener créditos u otros beneficios, cometer conductas delictivas o de lucro, o generar un daño patrimonial o moral, para sí o para otro.</p> <p data-bbox="500 869 954 1058">Se impondrá una pena de tres a diez años de prisión y de cuatrocientos a seiscientos días UMA diaria de multa y, en su caso, la reparación del daño que se hubiere causado.</p> <p data-bbox="500 1117 954 1306">Se aplicará la misma pena a quien otorgue su consentimiento para llevar a cabo la usurpación de su identidad, en cualquiera de las modalidades previstas en el párrafo anterior.</p>

	<p>Las penas aumentarán hasta en una mitad cuando:</p> <ol style="list-style-type: none">I. La víctima sea una persona con discapacidad o una persona mayor de sesenta años;II. Si la víctima es una niña, niño o adolescente;III. La persona responsable sea depositaria de información personal y la facilite a un tercero para llevar a cabo la usurpación;IV. El autor sea servidor público y la conducta la realice en ejercicio de sus funciones; oV. El sujeto activo se valga de la homonimia, parecido físico o similitud de voz para consumir la usurpación de identidad.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Por lo anteriormente expuesto y fundado, sometemos a la consideración del pleno la siguiente iniciativa con carácter de

Decreto

Único . - Se adiciona el Título Vigésimo Séptimo al Libro Segundo y el artículo 430 al Código Penal Federal en materia de usurpación de identidad, para quedar como sigue:

Título Vigésimo Séptimo Delitos contra la identidad de las personas

Capítulo Único Usurpación de identidad

Artículo 430.- Comete el delito de usurpación de identidad la persona que, por cualquier medio, incluyendo el uso de nuevas tecnologías digitales, se atribuya, suplante, apropie o utilice la identidad de otra persona, con la finalidad de acceder a recursos, obtener créditos u otros beneficios, cometer conductas delictivas o de lucro, o generar un daño patrimonial o moral, para sí o para otro.

Se impondrá una pena de tres a diez años de prisión y de cuatrocientos a seiscientos días UMA diaria de multa y, en su caso, la reparación del daño que se hubiere causado.

Se aplicará la misma pena a quien otorgue su consentimiento para llevar a cabo la usurpación de su identidad, en cualquiera de las modalidades previstas en el párrafo anterior.

Las penas aumentarán hasta en una mitad cuando:

- I. La víctima sea una persona con discapacidad o una persona mayor de sesenta años;
- II. Si la víctima es una niña, niño o adolescente;
- III. La persona responsable sea depositaria de información personal y la facilite a un tercero para llevar a cabo la usurpación;
- IV. El autor sea servidor público y la conducta la realice en ejercicio de sus funciones; o
- V. El sujeto activo se valga de la homonimia, parecido físico o similitud de voz para consumir la usurpación de identidad.

Transitorios

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

Artículo Segundo. Las legislaturas de las entidades federativas deberán, en el ámbito de sus respectivas competencias, realizar las adecuaciones normativas necesarias a fin de armonizar su legislación penal con lo dispuesto en el presente decreto, en un plazo no mayor a 180 días naturales contados a partir de la entrada en vigor del mismo.

Notas

1 Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. New York University Press. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899131

2 Proofpoint (2025). Email Spoofing: qué es, cómo funciona y cómo prevenirlo. Proofpoint. Disponible en: <https://www.proofpoint.com/es/threat-reference/email-spoofing>

3 IBM. (2025) Ingeniería social. Disponible en: <https://www.ibm.com/es-es/topics/social-engineering>

4 Guerra Valdivia, A. R. (2020). La identidad en la era digital. Revista Mexicana de Ciencias Penales. Disponible en: <https://revistacienciasinacipe.fgr.org.mx/index.php/02/article/view/95/96>

5 Federal Trade Commission (2022), Acuerdo por violación de datos de Equifax. Disponible en: <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>

6 Europol, UNICRI, & Trend Micro (2020). Malicious uses and abuses of artificial intelligence. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

7 Lewis, J. A. (2018). Economic Impact of Cybercrime – No Slowing Down. Center for Strategic and International Studies (CSIS). Disponible en: <https://www.realinstitutoelcano.org/analisis/ciberseguridad-economica/#:~:text=En%20su%20Informe%20de%202018,%2C8%25%20del%20PIB%20mundial.>

8 Infobae (2020), Cinco formas de prevenir la clonación y el robo de identidad en tarjetas de crédito. Disponible en: [https://www.infobae.com/america/mexico/2020/01/29/cinco-formas-de-prevenir-la-clonacion-y-el-robo-de-identidad-en-tarjetas-de-credito/#:~:text=En%20este%20caso%2C%20Banxico%20inform%C3%B3,la%20tarjeta%20bancaria%20\(53%25\).](https://www.infobae.com/america/mexico/2020/01/29/cinco-formas-de-prevenir-la-clonacion-y-el-robo-de-identidad-en-tarjetas-de-credito/#:~:text=En%20este%20caso%2C%20Banxico%20inform%C3%B3,la%20tarjeta%20bancaria%20(53%25).)

9 Arreola González, J. I. R. (2021). Delito de Usurpación de Identidad. Disponible en: <https://sistemabibliotecario.scjn.gob.mx/sisbib/2018/000296181/000296181.pdf>.

10 Guerra Valdivia, Op. Cit.

11 La Jornada (2025), IA dispara riesgo de fraudes financieros y robo de identidad en México. Disponible en: <https://www.jornada.com.mx/noticia/2025/04/20/economia/advierte-cecoban-riesgo-de-fraudes-bancarios-mediante-ia#:~:text=M%C3%A9xico%20ocupa%20el%20octavo%20lugar,de%20la%20Ciudad%20de%20M%C3%A9xico.>

12 Derivado del análisis, las entidades federativas que carecen de una regulación expresa que sancione la usurpación de identidad son: Colima, Chiapas, Guerrero, Puebla y Yucatán.

Palacio Legislativo de San Lázaro, a 28 de abril de 2025

Diputada Claudia Alejandra Hernández Sáenz (rúbrica)