CÁMARA DE DIPUTADOS
LXVI LEGISLATURA
SOBERANÍA Y JUSTICIA SOCIAL

Gaceta Parlamentaria

Año XXIX | Palacio Legislativo de San Lázaro, miércoles 1 de julio de 2026 | Número 7072-II

CONTENIDO

Anexo II

Miércoles 1 de julio

01 JUL. 2026 SE TURNÓ A LA COMISIÓN DE JUSTICIA DE LA CÁMARA DE DIPUTADOS.

CÁMARA DE DIPUTADOS
LXVI LEGISLATURA
SOBERANÍA Y JUSTICIA SOCIAL

MARCELO DE JESÚS TORRES COFIÑO
DIPUTADO FEDERAL

Con proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal, en materia de robo y suplantación de identidad digital, violencia digital extorsiva y cobranza digital abusiva, a cargo del Diputado Marcelo de Jesús Torres Cofiño y suscrita por las y los Diputados del Grupo Parlamentario del Partido Acción Nacional

El suscrito, diputado federal **Marcelo de Jesús Torres Cofiño**, así como las y los diputados del Grupo Parlamentario del Partido Acción Nacional de la LXVI Legislatura de la Cámara de Diputados del Honorable Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; y el artículo 6, numeral 1, fracción I; 77; 78 y demás aplicables del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente Iniciativa con proyecto de decreto por el que se adiciona un Capítulo II Bis al Título Noveno del Libro Segundo, denominado: "Robo y suplantación de identidad digital y de la violencia digital extorsiva" que comprende los artículos 211 bis 8, 211 bis 9, 211 bis 10, 211 bis 11 y 211 bis 12, todos del Código Penal Federal, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

En México, el teléfono celular se ha convertido en la puerta de entrada a la vida personal, familiar, financiera y laboral de millones de personas. Desde ese dispositivo se administran cuentas bancarias, se gestionan créditos, se mantiene comunicación con la familia y se resguardan fotografías, documentos y datos sensibles.

Esta centralidad del celular ha sido aprovechada por la delincuencia para abrir una nueva frontera del crimen: el hackeo de cuentas, el robo de identidad digital y la extorsión mediante aplicaciones de préstamo y plataformas de cobranza digital.

La realidad es brutal:

- El robo de identidad y los fraudes derivados de él han crecido de forma explosiva. De acuerdo con datos recientes, los fraudes por robo de identidad a clientes bancarios en México sumaron más de 11 mil millones de pesos en un solo año.

- Informes especializados señalan que el robo de identidad digital aumentó alrededor de 84 % en 2024, con pérdidas estimadas superiores a los 14 mil millones de pesos, impulsado por el crecimiento del comercio electrónico y los servicios digitales.

Estas cifras no son frías estadísticas: detrás de cada caso hay una persona a la que le vaciaron su cuenta, le negaron un crédito, la señalaron como "deudora morosa" o incluso como "delincuente" ante sus contactos, sin haber cometido delito alguno.

Un capítulo especialmente grave lo constituyen las aplicaciones de préstamo conocidas como "montadeudas".

La Secretaría de Seguridad y Protección Ciudadana y diversas policías cibernéticas han documentado el modus operandi de estas apps:

1. Ofrecen préstamos "fáciles y rápidos" mediante publicidad engañosa.

2. Obligan al usuario a otorgar permisos amplísimos sobre su celular: acceso a contactos, fotos, cámara, micrófono y ubicación.

3. Imponen intereses usureros y plazos imposibles de cumplir.

4. Cuando el usuario no puede pagar de inmediato, despliegan una campaña de acoso y violencia digital, a través de diversas acciones de intimidación que van subiendo de nivel, entre estas se pueden mencionar las siguientes:

- Difamación.
- Envío masivo de mensajes a los contactos.
- Manipulación de imágenes.
- Amenazas de muerte o de agresiones.
- Acusaciones falsas de pedofilia, secuestro, estafa, o "deudor moroso exhibido".

Datos del Consejo Ciudadano y de la CONDUSEF dan cuenta de más de mil aplicaciones reportadas bajo este modus operandi entre 2021 y 2024, muchas de ellas activas en tiendas digitales o en archivos APK distribuidos por redes sociales.

No se trata únicamente de un problema financiero. Es una forma de violencia digital extorsiva que destruye la salud mental y la reputación de las personas, y que, en muchos casos, alcanza a sus círculos familiares, laborales y comunitarios.

Paralelamente, el hackeo de redes sociales, cuentas de mensajería y correos electrónicos se ha vuelto cotidiano. En su momento, el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emitió diversas guías y recomendaciones para que las personas protegieran sus

redes, cambiaran contraseñas, activaran el doble factor de autenticación y denunciaran el uso indebido de sus datos.[1]

Por su parte, el 30 de junio de 2025, la Secretaría de Seguridad y Protección Ciudadana publicó un Comunicado en el que emitió recomendaciones de seguridad en el contexto del Día Mundial de las Redes Sociales, y destaca que los ciberdelincuentes aprovechan la información compartida en redes para la creación de perfiles falsos. En ese sentido recomienda: ajustar la configuración de privacidad de las cuentas, definir quién puede ver las publicaciones, enviar mensajes o etiquetar; y evitar compartir información personal o sensible, como son dirección, número de teléfono, escuela, lugar de trabajo o rutinas diarias, entre otras.[2]

Sin embargo, la realidad es que, aun siguiendo todas las recomendaciones, el marco penal federal no contempla un delito autónomo de robo y suplantación de identidad digital. En la práctica, se busca equiparar la conducta dentro de figuras como el fraude, el acceso ilícito a sistemas informáticos o la falsificación de documentos, lo que dificulta la persecución y deja a la víctima en estado de indefensión, sobre todo cuando:

- Alguien abre cuentas bancarias a su nombre.
- Contrata servicios o créditos utilizando su identidad.
- Opera en plataformas financieras y redes sociales simulando ser la persona afectada.
- Utiliza esa suplantación para extorsionar, difamar o cometer otros delitos.

Este vacío normativo contrasta con la magnitud del problema: según el sitio "unico", "Red Colectiva Contra el Fraude", tan solo en 2024, el fraude por suplantación digital creció un 84% y la circulación de identidades falsas un 49%, de acuerdo con el informe A Year in Fraud.[3] México se ha convertido en el epicentro del fraude digital en Latinoamérica, con niveles cinco veces más altos que países como Brasil.[4]

Por otro lado, datos de la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) revelan que los delitos asociados al robo de identidad física también están en ascenso: las denuncias por créditos fraudulentos mediante identidad robada crecieron 110% entre 2021 y 2024; y los documentos más

[1] INAI (2018). Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital. Consultado en línea el 18 de noviembre de 2025. https://inicio.inai.org.mx/GuiasTitulares/5RecomendacionesPDP_Web.pdf
[2] Información consultada en línea el 18 de noviembre de 2025. https://www.gob.mx/sspc/prensa/la-sspc-emite-recomendaciones-de-seguridad-en-el-dia-mundial-de-las-redes-sociales?idiom=es
[3] Informe en línea: https://25849394.hs-sites-eu1.com/es/a-year-in-fraud
[4] Información recuperada en línea: https://www.unicoid.mx/post/robo-de-identidad-critico-en-mexico

falsificados incluyen la INE (32%), comprobantes de domicilio (28%) y títulos profesionales (15%).

Si bien la protección legal existe, está fragmentada, desactualizada y sin "dientes" suficientes frente a un fenómeno que opera 24/7 y a escala masiva. La víctima debe moverse en un verdadero laberinto institucional, por ejemplo:

- Código Penal Federal y códigos penales locales: prevén delitos informáticos, extorsión, amenazas, coacción, calumnia, etc., pero sin una figura específica para la identidad digital ni para la violencia digital extorsiva ligada a apps de préstamo.

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares: establece obligaciones para empresas en el tratamiento de datos personales y prevé sanciones administrativas, pero no regula de forma expresa la prohibición del uso de contactos y datos de terceros para prácticas de cobranza digital abusiva ni prevé medidas cautelares inmediatas para detener el daño.

- Normatividad financiera y de protección al consumidor: CONDUSEF y Profeco pueden sancionar malas prácticas, pero muchas aplicaciones son clandestinas, transfronterizas o cambian de nombre con frecuencia, lo que dificulta su sujeción al marco regulatorio.

La presente iniciativa se sustenta en diversos mandatos constitucionales y convencionales. El artículo primero de la Constitución Política establece la obligación de todas las autoridades de promover, respetar, proteger y garantizar los derechos humanos, entre ellos: la honra, la reputación, la integridad personal, el libre desarrollo de la personalidad y la protección de datos personales.

El artículo sexto constitucional prevé el derecho de acceso a la información y protección de datos personales. El artículo 16 el derecho a la inviolabilidad de las comunicaciones privadas y protección de datos personales. El artículo 17 estipula el derecho de acceso a la justicia pronta, completa e imparcial; y el artículo 20 contempla los derechos de las personas víctimas de delito.

Además, México está obligado por instrumentos jurídicos como la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, que consagran el derecho a la vida privada, a la honra y a la protección contra injerencias arbitrarias o abusivas en la vida privada y en la correspondencia.

La identidad digital es hoy una extensión de la identidad personal. Protegerla no es una opción, es una exigencia mínima de un Estado democrático y de derecho.

Frente a este panorama, la presente iniciativa tiene dos objetivos centrales:

1. Tipificar como delito federal el robo y suplantación de identidad digital, con sanciones proporcionales y agravantes específicas.

2. Tipificar la violencia digital extorsiva asociada a aplicaciones de préstamo y prácticas de cobranza digital abusiva, reconociendo su carácter de violencia económica, psicológica y reputacional.

Adicionalmente, se propone un mandato para que el Ejecutivo Federal, en coordinación con fiscalías, policías cibernéticas y autoridades de protección de datos, establezca un Protocolo Nacional de Respuesta Rápida para víctimas de robo de identidad y violencia digital.

Por lo anteriormente expuesto, someto a la consideración de esta honorable asamblea la siguiente Iniciativa con Proyecto de:

DECRETO

Artículo Único. Se adiciona un Capítulo II Bis al Título Noveno del Libro Segundo, del Código Penal Federal, denominado: "Robo y suplantación de identidad digital y de la violencia digital extorsiva" que comprende los artículos 211 bis 8, 211 bis 9, 211 bis 10, 211 bis 11 y 211 bis 12, para quedar como sigue:

CAPITULO II BIS
Robo y suplantación de identidad digital y de la violencia digital extorsiva

Artículo 211 bis 8.- Para los efectos de este Capítulo se entenderá por:

I. Identidad digital: conjunto de datos, credenciales, atributos, identificadores y elementos de autenticación electrónicos o digitales asociados a una persona física, que permiten identificarla o individualizarla en medios electrónicos, telemáticos o informáticos, incluyendo, de manera enunciativa mas no limitativa, nombres de usuario, contraseñas, tokens, datos biométricos, direcciones de correo electrónico, números telefónicos, identificadores de dispositivos, perfiles en redes sociales, cuentas de mensajería instantánea y credenciales digitales de autenticación.

II. Robo de identidad digital: apropiación, adquisición, transferencia o utilización indebida de la identidad digital de una persona, con la finalidad de suplantarla total o parcialmente, realizar actos jurídicos, operaciones

financieras, comunicaciones, contrataciones o cualquier otra conducta que produzca efectos hacia terceros o hacia la propia víctima.

III. Aplicaciones de préstamo o cobranza digital: programas informáticos, plataformas o aplicaciones móviles que ofrecen u operan créditos, préstamos, financiamientos o servicios de cobranza mediante medios electrónicos, ya sea que se encuentren o no debidamente autorizados por la legislación financiera aplicable.

IV. Violencia digital extorsiva: toda acción u omisión realizada mediante tecnologías de la información y comunicación, redes sociales, plataformas digitales o dispositivos electrónicos, que tenga por objeto intimidar, coaccionar o presionar a una persona para la obtención de un beneficio económico o para forzar la realización u omisión de un acto, mediante amenazas, difamación, calumnias, manipulación de imágenes, difusión de información personal o de contactos, reales o falsas.

Artículo 211 bis 9.- Se impondrá pena de tres a ocho años de prisión y de trescientos a seiscientos días multa a quien, por sí o por interpósita persona:

I. Sin consentimiento de la persona titular y con la finalidad de suplantarla, obtenga, transfiera, posea, venda, distribuya, entregue o utilice su identidad digital para realizar actos jurídicos, operaciones financieras, contrataciones, compras, movimientos en cuentas, apertura de créditos, obtención de servicios o cualquier otra operación que pueda generar obligaciones, cargos o afectaciones patrimoniales o reputacionales a la víctima;

II. Utilice la identidad digital de otra persona para acceder a sus cuentas, perfiles o sistemas de información, y desde éstos realice comunicaciones, publicaciones o instrucciones que puedan generar efectos jurídicos, económicos o reputacionales hacia la víctima o hacia terceros, y

III. Cree o utilice perfiles, cuentas, sitios web o identidades digitales falsas, utilizando datos reales o suficientes para confundir a terceros respecto de la identidad de la víctima, con el propósito de realizar fraudes, extorsiones, amenazas, acoso o difamación.

Las penas previstas en este artículo se incrementarán en una mitad cuando:

a) La conducta se cometa en perjuicio de personas adultas mayores, niñas, niños, adolescentes, personas con discapacidad o en situación de vulnerabilidad;

b) La conducta sea realizada por servidores públicos, empleados o prestadores de servicios de instituciones financieras, tecnológicas, de telecomunicaciones o de tratamiento de datos personales, aprovechando la información a la que tengan acceso, y

c) La conducta se cometa de manera reiterada o sistemática en contra de varias víctimas.

Artículo 211 bis 10.- Se impondrá pena de cuatro a diez años de prisión y de cuatrocientos a ochocientos días multa a quien:

I. Suplante la identidad digital de una persona para dirigirle amenazas, coacciones o exigencias económicas, o para dirigirlas a sus familiares, contactos o entorno laboral;

II. Utilice la identidad digital de una persona para difundir o publicar, ante terceros o en espacios de acceso público, mensajes, imágenes, audios o contenidos que le atribuyan falsamente la comisión de delitos, conductas deshonrosas o deudoras, con el fin de presionarla para realizar pagos, entregar documentos o realizar cualquier acto en contra de su voluntad, y

III. Amenace con difundir o difunda contenidos falsos, manipulados o descontextualizados, utilizando la identidad digital de la víctima o sus contactos, con la finalidad de obtener una ventaja económica o patrimonial.

Cuando las conductas anteriores se realicen a través de tecnologías de la información y comunicación de manera masiva, utilizando sistemas automatizados de envío o difusión de mensajes, las penas se incrementarán hasta en una mitad.

Artículo 211 bis 11.- Se le impondrá pena de cinco a doce años de prisión y de quinientos a mil días multa, sin perjuicio de las sanciones que correspondan por otros delitos que resulten, a quien:

Por medio de aplicaciones de préstamo o de cobranza digital, por sí o a través de terceros:

I. Recolecte, acceda o utilice, sin el consentimiento expreso, libre e informado de la persona usuaria, los contactos, archivos, imágenes, audios, videos, ubicación u otros datos almacenados en el dispositivo electrónico, con el fin de presionar el pago de deudas reales o supuestas;

II. Amenace con difundir, o difunda efectivamente, mensajes, imágenes, audios, etiquetas, calificaciones o cualquier otro contenido dirigido a los

contactos de la víctima, atribuyéndole la condición de deudor moroso, ratero, delincuente, pedófilo o cualquier otro calificativo que menoscabe su honra o reputación, con el fin de forzar el pago de cantidades de dinero, y

III. Manipule o altere imágenes o datos personales de la víctima para simular conductas delictivas, sexuales, violentas o deshonrosas, y amenace con difundirlas o las difunda para presionarla económicamente.

Las penas previstas en este artículo se incrementarán hasta en una mitad cuando:

a) Las conductas se realicen respecto de deudas cuyo monto original sea igual o inferior a doscientas veces el valor diario de la Unidad de Medida y Actualización;

b) Las conductas se cometan en perjuicio de varias personas utilizando la misma aplicación, plataforma o esquema, y

c) Las conductas involucren la creación de grupos, páginas o perfiles con el único propósito de exhibir, acosar o difamar a deudores, reales o supuestos.

Artículo 211 bis 12.- Ámbito de aplicación y cooperación internacional

Las conductas previstas en este Capítulo serán perseguibles como delitos de carácter federal cuando:

I. Se cometan utilizando redes públicas de telecomunicaciones, infraestructura informática o plataformas digitales cuya administración o efectos se extiendan a territorio nacional;

II. Produzcan efectos en personas residentes en México, independientemente del país desde cuya infraestructura se hayan realizado las conductas;

III. Involucren el uso, tratamiento o transferencia de datos personales de personas situadas en territorio nacional.

En estos casos, las autoridades federales competentes deberán establecer mecanismos de cooperación con las autoridades de otros Estados, así como con empresas proveedoras de servicios digitales, para la identificación de responsables, la preservación de evidencias digitales, el bloqueo de cuentas, aplicaciones o sitios web, y la eliminación de contenidos ilícitos.

Transitorios

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

Segundo. El Ejecutivo Federal, por conducto de las dependencias competentes, deberá realizar las adecuaciones reglamentarias necesarias para la correcta aplicación del presente Decreto, en un plazo no mayor a ciento ochenta días naturales contados a partir de su entrada en vigor.

Tercero. En un plazo no mayor a ciento veinte días naturales, contados a partir de la entrada en vigor del presente Decreto, el Ejecutivo Federal, en coordinación con la Fiscalía General de la República, las fiscalías de las entidades federativas, las instancias de seguridad pública, las autoridades de protección de datos personales y las autoridades financieras y de protección al consumidor, deberá emitir un Protocolo Nacional de Respuesta Rápida para Víctimas de Robo y Suplantación de Identidad Digital, Violencia Digital Extorsiva y Cobranza Digital Abusiva, que contendrá al menos:

I. Mecanismos de recepción de denuncias y reportes en tiempo real;

II. Canales de coordinación inmediata con policías cibernéticas;

III. Lineamientos para la preservación de evidencias digitales;

IV. Procedimientos para solicitar el bloqueo, suspensión o eliminación de contenidos ilícitos en plataformas digitales, y

V. Medidas de atención, acompañamiento y orientación a las víctimas.

Cuarto. En un plazo de sesenta días naturales, contados a partir de la entrada en vigor de este Decreto, las autoridades competentes deberán llevar a cabo campañas permanentes de información y prevención sobre los riesgos del robo de identidad digital, el uso de aplicaciones de préstamos irregulares y las prácticas de cobranza digital abusiva, así como sobre los derechos y vías de protección de las personas usuarias.

Dado en el Salón de Sesiones de la Comisión Permanente, a 01 de julio de 2026.

Dip. Marcelo de Jesús Torres Cofiño