



III LEGISLATURA

**CIUDAD DE MÉXICO A 10 DE SEPTIEMBRE DE 2024**

**DIP. MARTHA SOLEDAD ÁVILA  
VENTURA, PRESIDENTA DE LA MESA  
DIRECTIVA, DEL CONGRESO DE LA  
CIUDAD DE MÉXICO, III LEGISLATURA.**

**PRESENTE**

Honorable Congreso de la Ciudad de México:

La que suscribe **Diputada Ana Luisa Buendía García**, integrante del Grupo Parlamentario de MORENA del Congreso de la Ciudad de México, III Legislatura, con fundamento en lo dispuesto por los artículos 122 Apartado A, fracciones I y II párrafo cinco, de la Constitución Política de los Estados Unidos Mexicanos; Artículos 29 Apartado D, inciso a), y 30 numeral 1, inciso b), ambos de la Constitución Política; Artículos 12 fracción II, y 13 fracción LXIV de la Ley Orgánica del Congreso; Artículos 5 fracciones I y II, 82, 95 fracción II y 96 del Reglamento del Congreso, todos ordenamientos de esta Ciudad de México, someto a consideración del Pleno la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL ARTÍCULO 211 TER Y UN PÁRRAFO AL ARTÍCULO 334, AMBOS AL CÓDIGO PENAL PARA EL DISTRITO FEDERAL, A FIN DE AGRAVAR LA USURPACIÓN DE IDENTIDAD A TRAVÉS DEL EMPLEO DE TECNOLOGÍAS DE LA INFORMACIÓN E INTELIGENCIA ARTIFICIAL** lo anterior al tenor de las siguientes consideraciones:



III LEGISLATURA

## **EXPOSICIÓN DE MOTIVOS**

El avance tecnológico, aunque facilita nuestra vida cotidiana en muchos aspectos, también exige al Derecho Penal la comprensión, atención y sanción de conductas antijurídicas relacionadas con la informática y los medios electrónicos. La doctrina del Derecho de la Informática ha identificado tres alternativas para abordar los problemas jurídicos que plantea la sociedad informatizada: 1) la actualización de la legislación, 2) la evolución jurisprudencial, y 3) la redacción de leyes específicas.

En la actualidad, se han manifestado diversos delitos íntimamente relacionados con las tecnologías de la información y comunicación, los cuales se incrementan año con año debido a la falta de normas específicas que persigan estas conductas. En este sentido, la presente iniciativa busca evidenciar las lagunas legales existentes frente a lo que hoy se denomina ciberdelincuencia, en particular la usurpación de identidad y el hackeo de dispositivos móviles, así como proponer soluciones al respecto.

En primer lugar, es importante señalar que, desde hace algunos años, los delitos de "robo de identidad", "usurpación de identidad" y "falsificación de identidad y su uso indebido" han aumentado considerablemente a nivel mundial. De acuerdo con el Consejo Económico y Social (ECOSOC) de la Organización de las Naciones Unidas, la usurpación de identidad es el delito de más rápido crecimiento en el mundo, sin que existan acciones legislativas eficientes que atiendan a los usos y costumbres, y a la constante actualización de las tecnologías de la información.

En la capital de nuestro país este delito tiene su fundamento en el artículo 211 Bis del Código Penal, que para mayor referencia se cita a continuación:

### **"CAPÍTULO III**

#### **USURPACIÓN DE IDENTIDAD**

**ARTÍCULO 211 Bis.** - *Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.*

*Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo."*

No obstante, el robo de identidad a través del uso de la tecnología está en constante aumento. Según datos recientes del Banco de México y otras fuentes, el robo de identidad es un problema creciente en el país. Desde enero hasta septiembre de 2023, se registraron **26,175 casos** en el sistema bancario, con una afectación económica de **6,169 millones de pesos**<sup>1</sup>. Además, en 2022, las instituciones bancarias reportaron **78,788 denuncias** por este delito<sup>2</sup>.

---

<sup>1</sup> El Informador. (2024, junio 24). Robo de identidad en auge en México. El Informador. <https://www.informador.mx/economia/Robo-de-identidad-en-auge-en-Mexico-20240624-0038.html>

<sup>2</sup> Capital México. (2016). Cifras de robo de identidad en México. Capital México. <https://www.capitalmexico.com.mx/economia/cifras-robo-identidad-mexico-internet-identificacion-condusef-bancos/>

México ocupa el octavo lugar a nivel mundial en robo de identidad y el segundo en América Latina<sup>3</sup>. Las causas más comunes incluyen la pérdida de documentos (67%), el robo de carteras y portafolios (63%), y la obtención de información directamente de tarjetas bancarias (53%)<sup>4</sup>.

En el artículo "Robo de Identidad al acecho", publicado el 1 de julio de 2022 en la Revista de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)<sup>5</sup>, se menciona que, según la Asociación de Bancos de México (ABM), los casos de robo de identidad mediante la suplantación de páginas web de instituciones financieras aumentaron significativamente, siendo las personas adultas mayores las más vulnerables.

Esto se debe a que en 2021 se registraron 49,871 reclamaciones por este tipo de fraudes en la institución, lo que representa el 1% del total de quejas registradas ese año. Sin embargo, esto también indica un aumento del 54% en este tipo de estafas en comparación con el mismo periodo de 2020. A continuación, se cita el artículo de referencia para respaldar esta información:

*"...Robo de identidad al acecho*

*1 julio, 2022*

***Conoce "Alertas Buró" para evitar el fraude.***

*El avance tecnológico nos ha facilitado la vida en muchos aspectos, uno de ellos son las operaciones bancarias que hoy en día se pueden realizar sin la necesidad de salir de casa. Sin embargo, no todo es miel*

---

<sup>3</sup> Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (s.f.). Identidad Segura. Recuperado de [https://micrositios.inai.org.mx/identidadsegura/?page\\_id=45](https://micrositios.inai.org.mx/identidadsegura/?page_id=45)

<sup>4</sup> Ídem.

<sup>5</sup> Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2022, julio). Robo de identidad al acecho. Revista CONDUSEF. Recuperado de <https://revista.condusef.gob.mx/2022/07/robo-de-identidad-al-acecho/>

sobre hojuelas, ya que también se han modernizado los fraudes financieros y el robo de identidad.

### **Robo de identidad en aumento**

De acuerdo con la Asociación de Bancos de México (ABM), los casos de **robo de identidad**, a través de la suplantación de páginas digitales de las instituciones financieras, han tenido un crecimiento importante y son las personas adultas mayores, las más vulnerables.

El **robo de identidad** a este segmento de la población representa el 35% de los casos, y es que, según información de la ABM, este tipo de ataque está más enfocado en los usuarios que en las instituciones.

El registro de reclamaciones por este tipo de fraudes en la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), fue de 49 mil 871 en 2021, lo que representa el 1% del total de las quejas registradas en ese año; no obstante, representa un incremento del 54% sobre este tipo de estafa, respecto al mismo periodo del 2020.

De hecho, un estudio a nivel mundial de la compañía tecnológica Unisys, revela que las y los mexicanos son los más preocupados por el **robo de identidad** y el fraude de tarjetas bancarias, sobre todo aquellos con grado universitario.

Otros datos señalan que el 66% de las personas encuestadas desconfía de los enlaces sospechosos; solo el 29% de estas personas dijo conocer este tipo de estafas y otras que son más sofisticadas, como el secuestro SIM. Únicamente el 22% refirió conocer cuáles son las instituciones en las que puede presentar una denuncia en caso de ser víctima de fraude.

### **¿Cómo acceden a tu información?**

Es importante mencionar que el **robo de identidad** es un tipo de fraude que consiste en la obtención ilícita de los datos de otras personas, con el fin de cometer un delito a su nombre. Para complicar la situación, no es fácil de detectar, por lo que las víctimas se dan

*cuenta hasta que reciben llamadas o notificaciones de cobranza, o cuando les niegan solicitudes de crédito de manera imprevista.*

*De acuerdo con personas expertas en ciberseguridad, los ladrones de identidad pueden acceder a tu información a través de tres métodos: el phishing, que consiste cuando un estafador suplanta la identidad de un Banco o institución financiera y le notifica a la víctima, a través de correo electrónico, sobre supuestos movimientos inusuales en su cuenta bancaria. Casi siempre este correo va acompañado de una liga que lleva a páginas falsas y es donde solicitarán la información de cuentas personales, como claves y contraseñas.*

*Otra forma es mediante el vishing. Se trata de una llamada telefónica y funciona muy parecido al método anterior. El estafador se hace pasar por asesor bancario y te notifica de algún cargo no reconocido o de alguna otra irregularidad, como el que han pretendido utilizar tu cuenta y que es necesario cambiar contraseñas.*

*¡Cuidado! Ningún Banco pide contraseñas, códigos de confirmación o verificación por teléfono, ni cualquier otro dato. El tercer método es el smishing, el cual realizan por medio de mensajes de textos, donde te mandan alertas falsas o enlaces a sitios falsos de tu Banco para instalar un virus para obtener tus datos.*

### **¿Cómo prevenir este tipo de fraude?**

*Si bien los estafadores siempre buscarán formas nuevas de obtener tu información, lo cierto es que con las siguientes medidas podremos evitar ser víctimas de ellos:*

- Es muy importante que nunca proporciones información de tus cuentas bancarias por teléfono, correo electrónico, mensaje de texto o redes sociales, recuerda que ninguna institución financiera te solicitará tus datos.*
- Algunos Bancos ofrecen servicios de prevención y sistemas de alertas, como autenticación de doble factor, los cuales pueden ayudarte a detectar movimientos o cargos extraños en tu cuenta, por lo que te recomendamos que solicites a tu institución activar este servicio.*



III LEGISLATURA

- *Revisa de manera frecuente tus estados de cuenta.*
- *Evita dar clic a ligas o enlaces que te hagan llegar por mensajes, incluso si se trata supuestamente de tu banco. Si tienes dudas, lo mejor es que llames directamente al número oficial de tu institución bancaria.*
- *Procura generar contraseñas seguras, es decir, no elijas fechas de nacimiento, nombre de un familiar o mascota, etc.; y de preferencia incluye mayúsculas, minúsculas, números y caracteres especiales.*

*Además de los anteriores consejos, también puedes apoyarte de **"Alertas Buró"**, una herramienta de Buró de Crédito. Este servicio consiste en darte información y actualizar cambios importantes en tu reporte de crédito.*

*Con esta herramienta podrás recibir alertas cada vez que ocurra un movimiento, por ejemplo, si hiciste o no el pago de tu tarjeta, Alertas Buró te informará sobre ello, o en caso de que se registre un nuevo crédito en tu expediente te lo hará saber de inmediato, esto con la finalidad de que en caso de que no hayas sido tú, puedas reportarlo oportunamente.*

*En caso de que desees contratar este servicio debes tomar en cuenta lo siguiente: tiene un costo de 232 pesos de forma anual, puedes hacerlo desde el siguiente link: <https://www.burodecredito.com.mx/alertas-info.html> o a través de la app de Buró de Crédito. Para darte de alta deberás tener a la mano el estado de cuenta de tus tarjetas de crédito más recientes, crédito automotriz o hipotecarios (en caso de contar con alguno de ellos), ya que te solicitará dicha información.*

*Otros beneficios que te ofrece Alertas Buró, es que te enviarán cuatro "reportes Mi Buró", que incluye la información de todos tus créditos, cuatro "reportes Mi Score", para que conozcas la puntuación de tu comportamiento crediticio y protección de **robo de identidad**, los*



III LEGISLATURA

*365 días del año, además de que podrás monitorear en todo momento los cambios o consultas en tu historial crediticio...”*

Asimismo, de acuerdo con datos del Consejo Ciudadano para la Seguridad y la Justicia en 2023, el robo de identidad en México aumentó más del 200% en comparación con el año anterior. Este incremento se atribuye al auge del uso de la inteligencia artificial para cometer estos ilícitos. Este Consejo menciona que entre enero y octubre de este año se registraron 1,607 reportes por robo de identidad en el país, en contraste con los 505 del mismo periodo de 2022. Es decir, el aumento es del 218%, de acuerdo con el Consejo Ciudadano<sup>6</sup>.

Según el análisis del Consejo Ciudadano, durante el periodo estudiado, el 62% de los casos de robo de identidad reportados fueron resultado del hackeo de información en redes sociales, el 26% se debió al robo de información de teléfonos celulares, y el 2% a la clonación de tarjetas bancarias o falsificación de firmas.

Lo anterior quiere decir que en la medida que se ocupe la tecnología o bien, ahora la inteligencia artificial dentro del espacio delictivo, siempre habrá un riesgo e incremento de fraude, en razón de que la tecnología avanza considerablemente y engaña a las personas. Al respecto el Consejo ciudadano menciona por ejemplo que, los ciberdelincuentes solo necesitan un pequeño archivo de voz para generar frases y diálogos

---

<sup>6</sup> Palacios, S. (2023) El robo de identidad registró un aumento de más del 200% en este 2023. Consejo Ciudadano para la Seguridad y la Justicia. Recuperado de <https://www.altonivel.com.mx/mexico-en-alerta-por-aumento-del-200-en-robo-de-identidad-con-ia/>





enteros, en tanto que, con la alteración de imágenes o videos, se pueden crear circunstancias en las que la identidad de una persona es suplantada.

Es por lo anterior que, el delito de robo de identidad se utiliza ilegalmente para abrir cuentas de crédito, contratar líneas telefónicas, seguros de vida, realizar compras e incluso, en algunos casos, para cobrar seguros de salud y pensiones. En este contexto, la combinación de tecnología y usurpación de identidad demuestra que este delito se está extendiendo con mayor fuerza, especialmente debido a que la pandemia de COVID-19 obligó al sector público y privado a adoptar la tecnología para que los usuarios realicen operaciones o trámites en línea, acciones innovadoras que han llegado para quedarse, ya que antes generaban largas filas y horas de espera.

Sin embargo, debido al tipo de datos que se manejan, como datos personales, nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y seguridad social, y en la mayoría de los casos información financiera, se presentan mayores oportunidades para cometer ilícitos. Esto significa que hay más posibilidades técnicas y a distancia entre los sujetos activos y los sujetos pasivos, quienes a menudo se enteran mucho tiempo después, lo que también evidencia una falta de control y una clara necesidad de actualización legislativa en esta materia.

Como se ha mencionado anteriormente, el Código Penal Local no contempla sanciones específicas para delitos cometidos a través de tecnologías de la comunicación y telecomunicación, es decir, mediante el uso de programas informáticos o softwares de inteligencia artificial. Cabe destacar que hasta el momento, el único estado que ha abordado este tema es el Estado de San Luis Potosí, que el 26 de abril de 2019 aprobó

por unanimidad la reforma de su código penal para tipificar el delito contra la identidad de las personas cuando se atribuya por medios electrónicos, redes sociales o cualquier otro medio, la identidad de otra persona, o se otorgue su consentimiento para llevarlo a cabo, causando con ello un daño patrimonial, moral o algún lucro indebido, para sí o para otra persona. Por otro lado, en diversas entidades federativas se han presentado iniciativas para reforzar la ley penal, pero persisten la incomprensión y la omisión legislativa en este aspecto. Por ello, la Ciudad de México no debe ser la excepción en normar esta problemática.

Además de la usurpación de identidad mencionada anteriormente, es importante destacar otra conducta ilícita que está en aumento a nivel mundial: el “hacking” de dispositivos de comunicación, como teléfonos celulares, y en particular, el hacking de aplicaciones de mensajería y comunicación electrónica, como WhatsApp.

### **PROPUESTA DE SOLUCIÓN**

En virtud de los argumentos expuestos, esta iniciativa propone añadir dos disposiciones. La primera es un artículo 211 Ter, que agravaría hasta en tres cuartas partes las penas para quienes, sin el permiso de la persona legalmente autorizada, usurpen la identidad de otra utilizando tecnologías de la información, programas informáticos, software, hardware o cualquier otro medio tecnológico, ya sea directamente o a través de terceros. Esto implicaría que las penas para este delito, con la agravante propuesta, serían de 1 año 9 meses a 8 años 9 meses.



Asimismo, se propone añadir una agravante al artículo 334 para el delito de Violación de la Comunicación Privada. Esto se debe a que no solo se pueden robar cuentas de WhatsApp u otras aplicaciones para usurpar una identidad, sino también para obtener información. Por lo tanto, este artículo establece que las penas se incrementarán hasta en una tercera parte cuando, utilizando tecnologías de la información, programas informáticos, software, hardware o cualquier otro medio tecnológico, se acceda, desbloquee o intervenga teléfonos celulares, dispositivos de comunicación, aplicaciones electrónicas o equipos de cómputo sin el consentimiento de la persona legalmente autorizada. De esta manera, las penas se agravarían de la siguiente forma:

- A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de 2 años 8 meses a 10 años 8 meses, y
- A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrán de 4 a 16 años 4 meses.

En consecuencia, la propuesta quedaría de la siguiente manera:

### **CÓDIGO PENAL PARA LA CIUDAD DE MÉXICO**

<b>TEXTO VIGENTE</b>	<b>PROPUESTA DE ADICIÓN</b>
<b><i>(Sin correlativo)</i></b>	<b>ARTÍCULO 211 TER. - Las penas anteriores se aumentarán hasta en tres cuartas partes al que sin el permiso de quien</b>

	<p><b>legalmente deba otorgarlo y haciendo uso de tecnologías de la información, programas informáticos, software, hardware y cualquier otro medio tecnológico, por sí o por interpósita persona usurpe la identidad de una persona.</b></p>
<p><b>ARTÍCULO 334.</b> A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa. A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa.</p>	<p><b>ARTÍCULO 334.</b> A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa. A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa.</p> <p><b>Las penas anteriores se agravarán hasta en una tercera parte cuando haciendo uso de tecnologías de la información, programas informáticos, software, hardware y cualquier otro medio tecnológico, por sí o por interpósita persona acceda, desbloquee o intervenga teléfonos celulares o cualquier dispositivo de comunicación, aplicaciones</b></p>

	<b>electrónicas o equipos de cómputo sin el consentimiento de la persona que legalmente pueda otorgarlo.</b>
--	--

Con base en los razonamientos antes precisados, la suscrita Diputada, propone al Pleno de este Congreso de la Ciudad de México III Legislatura, la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL ARTÍCULO 211 TER Y UN PÁRRAFO AL ARTÍCULO 334, AMBOS AL CÓDIGO PENAL PARA EL DISTRITO FEDERAL, A FIN DE AGRAVAR LA USURPACIÓN DE IDENTIDAD A TRAVÉS DEL EMPLEO DE TECNOLOGÍAS DE LA INFORMACIÓN E INTELIGENCIA ARTIFICIAL**, para quedar de la siguiente manera:

### **DECRETO**

**ÚNICO.** Se adiciona el Artículo 211 TER y un tercer párrafo al Artículo 334 del Código Penal el Distrito Federal, para quedar como sigue:

**ARTÍCULO 211 TER.** - Las penas anteriores se aumentarán hasta en tres cuartas partes al que sin el permiso de quien legalmente deba otorgarlo y haciendo uso de tecnologías de la información, programas informáticos, software, hardware y cualquier otro medio tecnológico, por sí o por interpósita persona usurpe la identidad de una persona.



## CAPÍTULO IV

### VIOLACIÓN DE LA COMUNICACIÓN PRIVADA

**ARTÍCULO 334.** A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa.

A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa.

**Las penas anteriores se agravarán hasta en una tercera parte cuando haciendo uso de tecnologías de la información, programas informáticos, software, hardware y cualquier otro medio tecnológico, por sí o por interpósita persona acceda, desbloquee o intervenga teléfonos celulares o cualquier dispositivo de comunicación, aplicaciones electrónicas o equipos de cómputo sin el consentimiento de la persona que legalmente pueda otorgarlo.**

### TRANSITORIOS

**PRIMERO.** El presente Decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.



III LEGISLATURA

**ANA  
BUENDÍA**  
DIPUTADA LOCAL DTTO. 04  
GUSTAVO A. MADERO

**SEGUNDO.** Remítase a la Jefatura de Gobierno para su promulgación y publicación en la Gaceta Oficial de la Ciudad de México.

Dado en el Recinto del Congreso de la Ciudad de México, III Legislatura, a los diez días del mes de septiembre del año dos mil veinticuatro.

**ATENTAMENTE**



**DIP. ANA BUENDÍA GARCÍA**

**DISTRITO IV**