DIP. FAUSTO MANUEL ZAMORANO ESPARZA, PRESIDENTE DE LA MESA DIRECTIVA, DEL CONGRESO DE LA CIUDAD DE MÉXICO, II LEGISLATURA.

PRESENTE

El que suscribe **Diputado Nazario Norberto Sánchez**, integrante del Grupo Parlamentario de MORENA del Congreso de la Ciudad de México, II Legislatura, con fundamento en los artículos 122 apartado A, fracciones I y II párrafo 5 de la Constitución Política de los Estados Unidos Mexicanos; 29 Apartado D, inciso a) y 30 numeral 1, inciso b) de la Constitución Política de la Ciudad de México; 12 fracción II, y 13 párrafo primero de la Ley Orgánica del Congreso de la Ciudad de México; 5 fracciones I y II, 82, 95 fracción II y 96 todos del Reglamento del Congreso de la Ciudad de México, someto a consideración de este Pleno la **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 LA CIUDAD DE MÉXICO, A FIN DE AGRAVAR LA USURPACIÓN DE IDENTIDAD Y EL HACKEO DE TELÉFONOS CELULARES Y APLICACIONES ELECTRÓNICAS,** al tenor de las consideraciones siguientes:

I. Planteamiento del problema que se pretende resolver:

El avance tecnológico si bien es cierto a todos nos facilita nuestra vida cotidiana en muchos aspectos, también lo es que su crecimiento demanda al Derecho Penal la comprensión, atención y sanción de conductas antijurídicas en las que se ve inmersa la informática o todo medio electrónico. La doctrina del Derecho de la Informática, ha identificado tres alternativas de solución para hacer frente al problema jurídico que representa la sociedad informatizada, mismas que consisten

en: 1) la actualización de la legislación, 2) la evolución jurisprudencial; y, 3) la redacción de leyes de carácter particular.

En la actualidad ya se han manifestado diversos delitos que han tenido relación íntima con las tecnologías de la información y comunicación, delitos que se incrementan año con año, debido a que no hay norma que persiga estas conductas de manera especifcia. En ese sentido la presente iniciativa busca evidenciar la falta legal que existen frente a lo que hoy se denomina ciberdelincuencia con relación a la usurpación de identidad y el hackeo de móviles, y la propuesta de solución que el suscrito plantea.

En primer lugar, es importante señalar que desde hace algunos años el delito de *"robo de identidad*", *"usurpación de identidad", "falsificación de identidad y su uso indebido"*, ha aumentado considerablemente a nivel mundial, pues de conformidad 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 y que atiendan a los usos y costumbres, y la medida 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."

Sin embargo, el robo de identidad mediante uso de la tecnología va en aumento día con día, según datos del Banco de México desde el 2019 nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, el robo de identidad se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria.[1]

Ahora bien, el artículo *"Robo de Identidad al acecho"*[2], publicado el pasado 1 de julio del año en curso, en la Revista de la Comisión Nacional para la protección y defensa de los usuarios de servicios financieros mejor conocida como CONDUSEF, señala que, *"…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…"*

Lo anterior en virtud de que el registro de reclamaciones por este tipo de fraudes en esta institución, 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. Para robustecer lo anterior, se cita a continuación el artículo de referencia:

"…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

[1] La CONDUSEF alerta acerca del robo de identidad en México 26. De agosto de 2016. Sitio web: https://www.uv.mx/infosegura/general/noti_roboidentidad-13/

[2] Revista CONSUSEF. Robo de identidad al acecho. Sitio web: https://revista.condusef.gob.mx/wp-content/uploads/2022/06/robo_268.pdf

necesidad de salir de casa. Sin embargo, no todo es miel 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.

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

Sabemos que el delito de robo de identidad se usa de manera ilegal para abrir cuentas de crédito, contratar líneas telefónicas, seguros de vida, realizar compras e incluso, en algunos casos, para el cobro de seguros de salud y pensiones. En este

contexto, la mezcla de tecnología-usurpación de identidad demuestra que cada vez se extiende con mayor contundencia, y aún más derivado de que el COVID-19, obligó al sector público y privado a entrar al ámbito de la tecnología para que los usuarios realicen operaciones o trámites vía internet, acciones innovadoras que llegaron para quedarse, pues antes de ello generaban largar filas y horas de espera.

Empero, por el tipo de datos que se manejan como: datos personales, nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y seguridad social y la mayoría de veces información financiera; se presentan mayores oportunidades de cometer ilícitos, es decir mayores posibilidades técnicas y a distancia entre el o los sujetos activos contra los sujetos pasivos, toda vez que éstos últimos son los que se enteran mucho tiempo después, lo cual da lugar también a que no hay un control y en consecuencia una evidente falta de legislación y actualización de la materia.

Para esta forma de delinquir, como se ha expuesto anteriormente el código penal local no contempla una sanción cuando se realice a través de las tecnologías de la comunicación y la telecomunicación, es decir, mediante el uso de programas informáticos; cabe señalar que hasta el momento, el único estado que se ha pronunciado al respecto es el Estado de San Luis Potosí, toda vez que el 26 de abril de 2019, aprobó por unanimidad reformar el código penal del mismo, con el objeto de tipificar el delito contra la identidad de las personas a quien se le atribuya por medios electrónicos, redes sociales o cualquier otro medio, la identidad de otra persona u otorgue su consentimiento para llevarla a cabo usando 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, no obstante sigue persistiendo la incomprensión y la omisión legislativa en

este aspecto, en razón de ello, la Ciudad de México no debe ser la excepción para normar esta problemática.

Además de la usurpación de identidad señalada en los párrafos que preceden, es menester señalar otra conducta antijurídica que se encuentra en incremento a nivel mundial, esto es el "*hackeo*" de dispositivos de comunicación como teléfonos celulares o bien de manera particular el hackeo de aplicaciones electrónicas de mensajería y comunicación, por ejemplo, el What's app.

Al respecto, en noviembre del año próximo pasado, la Secretaría de Seguridad Ciudadana[3] de esta Capital, hizo de conocimiento a la Ciudadanía diversas recomendaciones para evitar el robo de cuentas de esta plataforma de mensajería, lo anterior en atención al monitoreo que realiza, así como las denuncias hechas por personas víctimas de este ilícito:

> *"Comunicado 2774*
>
> *Como resultado del constante monitoreo de la red pública de Internet, la Unidad de Policía Cibernética de la Secretaría de Seguridad Ciudadana (**SSC**) de la Ciudad de México, detectó denuncias ciudadanas que referían el robo de cuentas de los usuarios de la aplicación de mensajería WhatsApp.*
>
> ***Durante el trabajo de recopilación de datos, el patrullaje virtual y resultado de la atención a dichas denuncias ciudadanas, se pudo obtener información sobre este tipo de estafa, en la que el objetivo de los ciberdelincuentes es obtener una cuenta real de WhatsApp y poder suplantar la identidad de la víctima para obtener beneficios económicos por medio de depósitos a través de transferencias bancarias.***
>
> ***Posteriormente, el delincuente puede pedir en cualquier momento el acceso a tu cuenta de WhatsApp en otro dispositivo ajeno al tuyo, solo es necesario que el descargue la aplicación y cologue tu número, y si no***

[3] Comunicado 2774. Secretaría de Seguridad Ciudadana. Sitio web: https://www.ssc.cdmx.gob.mx/comunicacion/nota/2774-la-unidad-de-policia-cibernetica-de-la-ssc-y-meta-emiten-recomendaciones-para-evitar-el-robo-de-cuentas-de-whatsapp

cuentas con las medidas de seguridad adecuadas, podrá ingresar fácilmente y así obtener información personal.

Por lo que, la Unidad de Policía Cibernética de la SSC en coordinación con el proveedor del sevicio de WhatsApp, Meta, emiten las siguientes recomendaciones para los usuarios de esta aplicación:

- *Nunca compartas tu código de activación. Es el código de 6 dígitos que recibes por mensaje SMS.*
- *Establece un PIN personal para que tu cuenta esté doblemente protegida. Ve a Ajustes/Configuración > Cuenta > Verificación en dos pasos > Activar.*
- *Haz que tu foto de perfil solo sea visible para tus contactos. Ve a Ajustes /Configuración > Cuenta > Privacidad > Foto de perfil > Mis contactos.*
- *Si un familiar o amigo te hace un pedido inusual por WhatsApp, llama a la persona para confirmar su identidad.*

Si crees que alguien robó tu cuenta de WhatsApp, los dos pasos a seguir son los siguientes:

- *Envía un correo electrónico (en español) a support@whatsapp.com con tu número telefónico completo (incluyendo códigos de país y área), describiendo lo que sucedió. Recibirás una respuesta en un lapso no mayor a 48 horas.*
- *Mientras tanto, avisa lo sucedido a tus amigos y familiares.*
- *Obtén más información de estás medidas en faq.whatsapp.com.*

La SSC recuerda a las y los usuarios de la red pública de Internet, de redes sociales o cualquier otra aplicación, que, si es víctima de un delito, contacte a la ***Unidad de Policía Cibernética*** *al correo electrónico* ***policia.cibernetica@ssc.cdmx.gob.mx*** *o al teléfono* ***5242 5100 ext. 5086*** *y acuda a presentar su denuncia ante cualquier agente del Ministerio Público.*

De la misma manera, en el mes de enero de 2022, la Secretaría volvió a alertar mediante un comunicado[4] a la Ciudadanía sobre el aumento de robo de cuentas de whats app, mismo que se cita enseguida:

> *"…Comunicado 84*
>
> *La Unidad de Policía Cibernética de la Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México,* ***en atención a los reportes de usuarios de la aplicación de mensajería WhatsApp que refieren el robo de cuentas, exhorta a la ciudadanía a activar el código de verificación de dos pasos y denunciar cualquier incidente.***
>
> ***Con el robo de cuentas, los ciberdelincuentes lo que intentan es suplantar má identidad de la víctima para obtener beneficios económicos por medio de depósitos a través de transferencias bancarias, esto se detectó a través de los patrullajes virtuales y el monitoreo constante en la red pública de Internet.***
>
> ***Además, cuando el delincuente accede a la cuenta de WhatsApp, si esta no está debidamente protegida con las medidas de seguridad adecuadas, puede obtener información personal****, por ello la Unidad de Policía Cibernética emite las siguientes recomendaciones:*
>
> *• Nunca compartas tu código de activación. Es el código de 6 dígitos que recibes por mensaje SMS.*
>
> *• Establece un PIN personal para que tu cuenta esté doblemente protegida. Ve a Ajustes/Configuración > Cuenta > Verificación en dos pasos > Activar.*
>
> *Además, en colaboración con Meta, la SSC recomienda a los usuarios que otra medida de seguridad es hacer que la foto de perfil solo sea visible para los contactos, lo que se activa de la siguiente manera: Ve a Ajustes /Configuración > Cuenta > Privacidad > Foto de perfil > Mis contactos.*
>
> *Por otro lado, si crees que alguien robó tu cuenta de WhatsApp, los dos pasos a seguir son los siguientes:*

[4] Comunicado 84. Secretaría de Seguridad Ciudadana. Sitio web: https://www.ssc.cdmx.gob.mx/comunicacion/nota/84-la-ssc-traves-de-la-unidad-de-policia-cibernetica-exhorta-los-usuarios-de-la-aplicacion-whatsapp-activar-la-verificacion-en-dos-pasos-para-evitar-el-robo-de-sus-cuentas

• Envía un correo electrónico (en español) a support@whatsapp.com con tu número telefónico completo (incluyendo códigos de país y área), describiendo lo que sucedió. Recibirás una respuesta en un lapso no mayor a 48 horas.

• Mientras tanto, avisa lo sucedido a tus amigos y familiares.

Finalmente, si los usuarios de estas aplicaciones reciben llamadas supuestamente hechas por familiares o amigos en las que les hacen pedidos inusuales, lo más importante es llamar a la persona para confirmar su identidad y en caso de sospechar un delito, bloquear el contacto y denunciar el incidente.

Para más información de las medidas de seguridad que se pueden aplicar al sistema de mensajería instantánea WhatsApp para evitar ser víctima de un delito cibernético, la ciudadanía puede acceder al link faq.whatsapp.com.

La SSC recuerda a las y los usuarios de la red pública de Internet, de redes sociales y aplicaciones que, si es víctima de un delito, contacte a la Unidad de Policía Cibernética al correo electrónico policia.cibernetica@ssc.cdmx.gob.mx o al teléfono 5242 5100 ext. 5086 y acuda a presentar su denuncia ante cualquier agente del Ministerio Público…"

Esta problemática, como se ha expuesto ha aumentado considerablemente, incluso algunos medios de comunicación han denominado esta acción como una *"oleada de hackeo"* de miles de cuentas, por ejemplo, se cita la siguiente nota periodística publicada el pasado 10 de noviembre del año en curso:

"Oleada de hackeo de miles de cuentas de WhatsApp en Puebla para estafar con depósitos bancarios

Efraín Núñez.

noviembre 10, 2022

Miles de usuarios de la aplicación whatsapp han sido objeto en las últimas semanas de hackeo de sus cuentas, actividad que se intensifica en los últimos meses del año como se registró a principios de 2022.

En todos los casos la táctica de los hackers que se dedican a esta actividad es apoderarse de la cuenta del usuario y pedir entre 4 mil 500 y hasta 200 mil pesos prestados a nombre de este.

Los afectados de los que ha tenido cuenta este medio de comunicación han sido de diversos sectores, entre estos presidentes municipales, periodistas y del ámbito empresarial.

Pese a las afectaciones al patrimonio de las personas las empresas telefónicas se deslindan de los hackeos y es imposible hablar con algún representante de la aplicación, ya que la única forma de comunicarse con whatsapp es vía correo electrónico, donde se recomienda proteger la cuenta con una clave a dos pasos.

Uno de los casos más representativos es el de Rogelio López Angulo, presidente municipal de Huauchinango, quien en septiembre pasado posteó en sus redes sociales que su cuenta había sido hackeada.

"Quiero compartir con ustedes, que me hackearon mi whatsapp. No depositen nada a mi nombre por favor. Ayudemos a prevenir sobre este tema y evitar que más personas sean víctimas. ¡Gracias!", escribió en su cuenta de facebook.

Varios de sus contactos revelaron en los comentarios de su posteo que les solicitaron hasta 63 mil pesos a su nombre como préstamo, sin que ninguno de ellos hubiera caído en la estafa.

La mayoría de los usuarios se encuentran en grandes grupos de whatsapp que abren para compartir información relativa a su trabajo o para contactarse con conocidos y clientes.

***Los hackeos principalmente ocurren en los ciclos de fines de quincena**, en tanto que los hackers se están ubicando en países caribeños como República Dominicana, Jamaica y Haití donde operan los servidores para no ser detectados.*

A la par ocurre una oleada de extorsiones en las que se advierte que si no se paga cierta cantidad de dinero se amenaza con mandar ciertos contenidos a los contactos de whatsapp.

Otro de los casos más recientes correspondió a al menos dos trabajadores del ayuntamiento capitalino, una de las cuales tuvo que cambiar su número de móvil debido a que el teléfono se bloqueó.

La dueña de un spa recibió hace unas semanas advertencias de la propia empresa de whatsapp en el sentido de que alguien intentaba acceder a su cuenta, por lo que optó por poner la verificación en "dos pasos" para entrar a su chat.

En enero pasado, La Jornada de Oriente publicó que abrir una dirección enviada por un mensaje de texto, descargar una aplicación fuera de sitios reconocidos, proporcionar códigos de verificación, contestar llamadas y hasta dejar sin clave el buzón de voz, puede representar para una persona ser víctima de algún fraude de plataformas electrónicas conocidos como "ciberfraudes".

Datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros (Condusef) señalan que las reclamaciones por consumos vía internet no reconocidos y las transferencias electrónicas no reconocidas de 2019 a 2021, en el contexto de la epidemia de Covid–19, se han incrementado hasta en un 878 y 273 por ciento.

En tanto, Bárbara Sánchez, catedrática de la Facultad de Computación de la Universidad Autónoma de Puebla (UAP), reveló que las imágenes, videos y memes que se transmiten por whatsapp pueden contener virus para hackear los dispositivos."

Cabe señalar que incluso algunos de los Diputados y Diputadas que integramos esta Segunda legislatura, hemos sido víctimas de esta conducta y los delincuentes han solicitado favores y dinero usurpando nuestra identidad, nuestra investidura y nuestras cuentas de mensajería como es el caso del whats app.

II. Propuesta de Solución:

En razón de los argumentos antes precisados, en la presente iniciativa se pretende adicionar dos disposiciones, la primera se trata de un artículo 211 Ter para agravar 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**; esto quiere decir que las penas para este delito con la agravante que se proponen serán de **1 año 9 meses** a **8 años 9 meses.**

Al mismo tiempo, también se adiciona una agravante al artículo 334 para el delito de **Violación de la Comunicación Privada,** ya que no necesariamente pueden robar las cuentas de whats app, o cualquiera otra aplicación para robar una identidad sino para obtener información, de tal manera que, se establece en este artículo que las penas se incrementarán 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, de tal manera que las penas se agravarían de la siguiente manera:

- 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.**

Bajo ese tenor, la propuesta quedaría de la siguiente manera:

CÓDIGO PENAL PARA LA CIUDAD DE MÉXICO

TEXTO VIGENTE	PROPUESTA DE ADICIÓN
(Sin correlativo)	**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.**
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.	**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.

Con base en los razonamientos antes precisados, el suscrito Diputado propone al Pleno de este Congreso de la Ciudad de México, II 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 LA CIUDAD DE MÉXICO, A FIN DE AGRAVAR LA USURPACIÓN DE IDENTIDAD Y EL HACKEO DE TELÉFONOS CELULARES Y APLICACIONES ELECTRÓNICAS,** para quedar de la siguiente manera:

DECRETO

ÚNICO. Se adiciona el Artículo 211 TER y un tercer párrafo al Artículo 334 del Código Penal para la Ciudad de México, 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.

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

Dado en el Congreso de la Ciudad de México, a los 6 días del mes de diciembre de 2022.

ATENTAMENTE

Nazario Norberto Sánchez

DIP. NAZARIO NORBERTO SÁNCHEZ

DISTRITO IV.