INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UN ARTÍCULO 252 BIS AL CÓDIGO PENAL FEDERAL, PARA TIPIFICAR EL DELITO DE SUPLANTACIÓN DE IDENTIDAD Y SANCIONAR A QUIEN COMETA ESTE DELITO UTILIZANDO INTELIGENCIA ARTIFICIAL.

El que suscribe, **Senador Alejandro Moreno Cárdenas**, integrante del Grupo Parlamentario del Partido Revolucionario Institucional, de la LXVI Legislatura del H. Congreso de la Unión y con fundamento en lo dispuesto en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, así como por el artículo 8, numeral 1, fracción I del Reglamento del Senado de la República, someto a la consideración del Pleno, la siguiente Iniciativa con Proyecto de Decreto de acuerdo con la siguiente:

Exposición de Motivos

La suplantación de identidad y los fraudes cibernéticos son problemáticas cada vez más comunes en México, afectando a personas, empresas e instituciones. En la actualidad, los avances en la inteligencia artificial facilitan a los delincuentes suplantar la identidad mediante la clonación del rostro o la voz de cualquier persona, permitiendo crear frases o videos haciéndolos pasar como reales, generando afectaciones graves en las víctimas.

Según cifras del **Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México,** la usurpación de identidad mediante el uso de inteligencia artificial aumentó un 218 por ciento en el último año. Entre enero y octubre de 2023, se reportaron mil 607 casos de robo de identidad. De estos, el 62 por ciento se debió al hackeo de cuentas en redes sociales, el 26 por ciento al robo de información desde dispositivos móviles y el 2 por ciento a la clonación de tarjetas bancarias o falsificación de firmas[1].

Si bien, el desarrollo de la Inteligencia Artificial ha demostrado ser una herramienta poderosa que, cuando se utiliza adecuadamente, mejora la calidad de vida, la productividad y la eficiencia en muchas áreas. En manos equivocadas, la inteligencia artificial se convierte en una herramienta peligrosa para amplificar los delitos de suplantación de identidad. **La facilidad con la que los delincuentes pueden manipular videos, audios, datos y sistemas biométricos muestra que los riesgos asociados con la Inteligencia Artificial deben ser abordados de manera urgente**.

En el **Partido Revolucionario Institucional** estamos convencidos de la necesidad de contar con un Estado y una legislación que promueva y regule el desarrollo de la

[1] Comunicado INAI-373_23.pdf

inteligencia artificial de manera ética y responsable y sancione **su uso con fines de desprestigio y de usurpación de identidad.**[2]

Somos conscientes de que esta situación exige una respuesta por parte del Poder Legislativo, por ello, la presente iniciativa tiene como objetivo:

- Tipificar en el Código Penal Federal el delito de suplantación de identidad.

- Se establece que comete el delito de suplantación de identidad quien, sin consentimiento de la persona física o jurídica, se atribuya, apropie, transfiera o utilice la identidad de otro, con el fin de causar un daño, perjuicio o de obtener un lucro indebido, propio o para un tercero.

- Se propone como pena a quien cometa este delito, de dos a cinco años de prisión y de 200 a 1,000 unidades de medida y actualización, además de la reparación del daño.

- Se equipará el delito de suplantación de identidad a quien utilizando cualquier software o aplicación de inteligencia artificial, elabore, genere, distribuya o manipule imágenes, videos o audios con la intención de suplantar la identidad de una persona o hacer pasar dichos contenidos como reales.

- Se establece que se entenderá por software de inteligencia artificial cualquier sistema, dispositivo o programa informático que posea la capacidad de realizar actividades que, tradicionalmente, requieren de la inteligencia humana para su ejecución, incluyendo, entre otros, sistemas de procesamiento de lenguaje natural, aprendizaje automático, redes neuronales y algoritmos avanzados.

La suplantación de identidad un fenómeno que ha crecido exponencialmente con el auge de la digitalización y la globalización

La suplantación de identidad es un delito que puede ocurrir de diversas formas, incluyendo el uso no autorizado de datos personales, la clonación de tarjetas bancarias o incluso la creación de perfiles falsos para engañar a terceros. En México, los fraudes cibernéticos y la suplantación de identidad se han incrementado en los últimos años.

Las leyes deben contemplar sanciones específicas para los delitos cometidos con el uso de Inteligencia Artificial y promover una mayor cooperación entre los sectores público y privado para desarrollar soluciones tecnológicas más seguras. Asimismo, la capacitación y concienciación de los ciudadanos sobre los riesgos de la IA y cómo protegerse contra estos nuevos tipos de fraude son esenciales para mitigar el impacto de la suplantación de identidad en el futuro digital

[2] Ibidem

Según cifras de la Asociación de Internet MX, en 2023 el 72% de los mexicanos que utilizan internet han experimentado algún tipo de fraude o intento de fraude cibernético.

Las modalidades más comunes incluyen el robo de datos personales a través de correos electrónicos falsos (phishing), llamadas telefónicas fraudulentas (vishing) y sitios web clonados. La facilidad con la que se puede acceder a información personal en internet, sumada a la falta de una legislación robusta y de medidas de protección adecuadas, hace que los ciudadanos estén expuestos a este tipo de delitos.

Justo es reconocer que hemos avanzado en la creación de leyes y mecanismos para enfrentar los delitos cibernéticos. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, promulgada en 2010, es uno de los principales marcos legales que busca proteger la privacidad de los datos de las y los ciudadanos. Sin embargo, si bien esta ley es un paso importante, sigue siendo insuficiente para abordar de manera efectiva la complejidad de los delitos cibernéticos actuales, especialmente la suplantación de identidad.

Uno de los principales desafíos es la falta de claridad en la definición y sanción de los delitos relacionados con la suplantación de identidad. **Aunque el Código Penal Federal establece penas para el uso indebido de datos personales y la falsificación de documentos, no existe una regulación específica que aborde de manera integral el delito de suplantación de identidad y mucho menos la comisión de este delito en el contexto digital.**

Por otro lado, las autoridades enfrentan dificultades para rastrear y capturar a los delincuentes, muchos de los cuales operan desde el extranjero o utilizan tecnologías avanzadas para ocultar su identidad y ubicación.

Ante este panorama, es fundamental que México avance hacia una legislación más sólida y coherente que aborde específicamente la suplantación de identidad en el ámbito cibernético. La identidad es uno de los derechos más básicos de los ciudadanos, y su protección es esencial para garantizar la libertad y la privacidad de las personas.

Cuando alguien sufre suplantación de identidad, no solo se ve afectado en términos financieros, sino también en su reputación y dignidad personal. Una legislación adecuada debe garantizar que los ciudadanos tengan mecanismos efectivos para proteger su identidad y obtener justicia en caso de que sean víctimas de este delito.

En una era en la que las transacciones electrónicas y los servicios digitales son fundamentales para la economía, la confianza en la seguridad de estos sistemas es crucial. Los fraudes cibernéticos y la suplantación de identidad erosionan esa confianza, lo que puede tener consecuencias graves para la economía digital.

Si los ciudadanos y las empresas no confían en la seguridad de las plataformas en línea, es probable que limiten su uso, lo que afectaría el crecimiento de sectores como el comercio electrónico, la banca digital y otros servicios basados en internet y redes informáticas.

Es por ello que necesitamos avanzar en una reforma legal que avance en sancionar severamente la suplantación de identidad e inhiba estas conductas en el ecosistema digital de México.

La suplantación de identidad está directamente relacionada con diversos tipos de fraudes financieros, como el robo de cuentas bancarias, la obtención de créditos fraudulentos y la compra no autorizada de bienes y servicios.

Estos fraudes no solo afectan a las víctimas individuales, sino que también tienen un impacto significativo en las instituciones financieras y el sistema económico en su conjunto.

En esta evaluación contextual no puede quedar fuera una reflexión sobre lo que representó la pandemia de Covid19, la cual aceleró la adopción de herramientas y servicios digitales en México y en el mundo, lo que trajo consigo beneficios incuestionables, pero también expuso a las sociedades a una nueva ola de riesgos, entre ellos la suplantación de identidad y los fraudes cibernéticos.

La crisis sanitaria obligó a millones de personas y empresas a realizar una transición abrupta hacia el entorno digital, aumentando la dependencia de plataformas en línea para realizar compras, pagos, trámites gubernamentales y laborales. Este cambio, sin la debida preparación y sin medidas de seguridad robustas, abrió la puerta a una mayor actividad criminal en internet.

Con las restricciones de movilidad y el confinamiento, muchos ciudadanos que anteriormente no estaban familiarizados con las tecnologías digitales se vieron forzados a utilizarlas, lo que los convirtió en objetivos más vulnerables para los delincuentes cibernéticos.

Los estafadores se aprovecharon de la situación mediante tácticas como el phishing, suplantando instituciones de salud, bancos o agencias gubernamentales para obtener información personal y cometer fraudes. Además, el auge del comercio electrónico y las transacciones bancarias en línea aumentó exponencialmente durante la pandemia, lo que facilitó el acceso a datos financieros por parte de criminales con intenciones maliciosas.

El trabajo remoto, otra consecuencia de la pandemia, también incrementó la exposición a fraudes.

Muchas empresas implementaron soluciones improvisadas para continuar operando, sin contar con las infraestructuras de seguridad adecuadas.

Esto permitió a los ciberdelincuentes aprovechar vulnerabilidades en los sistemas de las organizaciones, suplantando la identidad de empleados o directivos para realizar fraudes internos o externos, como el robo de información confidencial o la desviación de fondos.

Con los avances tecnológicos actuales nos encontramos frente a la proliferación de diversas inteligencias artificiales. Debido al impacto que tienen, resulta importante su debida regulación, pues son una fuente de grandes efectos, tanto negativos como positivos. Las inteligencias artificiales se constituyen como herramientas, que pueden fungir para aspectos provechosos y benéficos, pero también pueden representar amenazas o riesgos.

Nuestro Instituto Político en su *Programa de Acción* ha enlistado algunos de estos riesgos fundamentales que surgen a raíz de la utilización de la inteligencia artificial, entre los que destacan:[3]

*1. **Desplazamiento de mano de obra y personal humano**. A raíz de la especialización de las diversas inteligencias artificiales, éstas pueden empezar a constituirse como opciones más atractivas para algunas empresas y organizaciones, en sustitución del empleo de personas.*

*2. **Comisión de delitos**. Se ha podido observar que las inteligencias artificiales tienen la posibilidad de ser usadas para los fines más diversos. Muchos de ellos han consistido en imitación de voz e imagen de las personas, lo que puede propiciar la comisión de delitos como el fraude o la suplantación de identidad.*

*3. **Conflictos en materia de propiedad intelectual y derechos de autor**. Como ya se comentó, las inteligencias artificiales son capaces, entre otras cosas, de copiar y reproducir la voz, estilo, redacción y diseño de diversas personalidades, incluyendo artistas, autores y/o creadores de contenido. Esta cualidad corre el riesgo de propiciar conflictos y controversias de índole legal pues los creadores originales quedan expuestos a la utilización de su imagen o incluso al plagio de sus obras.*

En contraparte, también afirmamos que: "***la inteligencia artificial puede ser una valiosa herramienta para los procesos gerenciales, para optimizar el manejo y procesamiento de datos, los procesos productivos, la toma de decisiones, para eficientar actividades, revolucionar las cadenas productivas y tecnológicas***".[4]

[3] https://pri.org.mx/ElPartidoDeMexico/Documentos/2024/ProgramadeAccion.pdf
[4] Ibidem

Marco Jurídico Nacional e Internacional

La Constitución Política de los Estados Unidos Mexicanos establece en su artículo 3º que:

> ***"Toda persona tiene derecho a gozar de los beneficios del desarrollo de la ciencia y la innovación tecnológica. El Estado apoyará la investigación e innovación científica, humanística y tecnológica, y garantizará el acceso abierto a la información que derive de ella, para lo cual deberá proveer recursos y estímulos suficientes, conforme a las bases de coordinación, vinculación y participación que establezcan las leyes en la materia; además alentará el fortalecimiento y difusión de nuestra cultura."***[5]

Asimismo, el artículo 6º de la mencionada Constitución Política de los Estados Unidos Mexicanos,[6] determina que:

> ***"Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión."***
>
> ***"El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet."***
>
> ***"La información que se refiere a la vida privada y los datos personales será protegida..."***

En el **marco internacional** encontramos los siguientes instrumentos y resoluciones:

- Capítulo 10 del Informe 2010 de la oficina de las Naciones Unidad contra la droga y el Delito, en materia de cibercrimen y robo de identidad.
- Consejo Económico y Social de la Organización de las Naciones Unidas, resolución 2004/26 en materia de falsificación de identidad.
- Convención de las Naciones Unidad contra la Delincuencia Organizada Trasnacional, en materia de fraude trasnacional vinculado en materia de robo de identidad.

Por lo que corresponde al **Código Penal Federal,** este no prevé la tipificación del delito de suplantación de identidad, sin embargo, en algunos **Códigos Penales Estatales si se sanciona este delito**, pero el tipo penal varía en cuanto a su alcance

[5] https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
[6] https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

y aplicación. Creando vacíos legales y desigualdades en la protección de las y los ciudadanos dependiendo de la región donde se encuentren.

En un estudio realizado por la Mtra. Mónica Márquez Tomás, denominado "Análisis del delito de usurpación de identidad en México"[7] analizó los códigos penales de las entidades federativas para identificar que Estados de la República contaban con el tipo penal y como se estructuraba, encontrando lo siguiente:

Entidad Federativa	Artículo del Código Penal Estatal
Aguascalientes	Artículo 181 A
Baja California	Artículo 175 quinquies
Baja California Sur	Artículo 363
Ciudad de México	Artículo 211 bis
Campeche	Artículo 242 bis
Colima	Artículo 224 bis
Coahuila	No tiene
Chiapas	Artículo 304 bis
Chihuahua	Artículo 206 Ter.
Durango	Artículo 175 bis
Estado de México	Artículo 264
Guanajuato	Artículo 214-A
Guerrero	No tiene
Hidalgo	**Artículo** 370
Jalisco	Artículo 143 QUÁTER
Michoacán de Ocampo	Artículo 301 bis
Morelos	Artículo 189 bis
Nayarit	Artículo 326
Nuevo León	Artículo 444
Oaxaca	Artículo 232 bis
Puebla	No tiene
Querétaro	No tiene
Quintana Roo	Artículo 195 SEXTIES
San Luis Potosí	Artículo 187 bis
Sinaloa	Artículo 177 bis
Sonora	Artículo 241 bis
Tabasco	No tiene
Tamaulipas	Artículo 263 bis
Tlaxcala	Artículo 282
Veracruz de Ignacio de la Llave	Artículo 283 bis.
Yucatán	No tiene
Zacatecas	Artículo 277 bis

***Dicho cuadro fue actualizado al 06 de octubre de 2024*

[7] Tomás, M. M. (s/f). *ANÁLISIS DEL DELITO DE USURPACIÓN DE IDENTIDAD EN MÉXICO*. Lasalle.mx. Recuperado el 6 de octubre de 2024, de https://repositorio.lasalle.mx/bitstream/handle/lasalle/1422/RA%2033%20Jul2019-335-368.pdf?sequence=1&isAllowed=y

La Mtra. Mónica Márquez al analizar los tipos penales en las entidades federativas, realiza las siguientes anotaciones:

- *En Aguascalientes, Baja California, Chiapas, Chihuahua, Guerrero, Puebla, Querétaro, Tabasco, Veracruz de Ignacio de la Llave y Yucatán sus Códigos Penales* no tipifican este delito.
- *En la mayoría de las legislaciones estatales se establece al sujeto activo como autor intelectual o material, al ejecutarlo cualquier persona, el tipo penal no exige calidad específica.*
- *El bien jurídico tutelado por la norma penal en general en las entidades son los siguientes: identidad, datos personales, cualquier tipo de datos y/o personalidad.*
- *En la mayoría de los tipos penales no se advierte una finalidad, en ocho de ellos se hace referencia a "fines ilícitos" o "fines de lucro", "la finalidad de obtener beneficios para si o para otro o el fin de perjudicar de algún modo al usurpado" y "cualquier fin", en general el fin debe ser ilícito y con la intención de perjudicar, al resultar importante como elementos de la usurpación de identidad el fin ilícito y la obtención de un beneficio.*
- *La consecuencia del delito se concreta en la sanción, esta puede ser penal y/o administrativa. La penal que establecen las entidades federativas, es variada, toda vez que, en tres de ellas la pena mínima es menor a un año, esto es, en Colima tres meses, en Quintana Roo y Sinaloa seis meses. La pena máxima es de ocho años en Durango, Jalisco y Nuevo León, y de siete años en Colima y Nayarit.*
- *Campeche, Colima, Hidalgo, Morelos y San Luis Potosí, mencionan "la reparación del daño causado"*
- *No existe una definición homogénea del delito de "usurpación de identidad", ni en los diccionarios, ni en la legislación nacional e internacional, es un delito que se encuentra en evolución en el que hace falta hacer mayores aportes.*
- *El delito de "usurpación de identidad" a nivel federal se encuentra aún con ausencia de un tipo penal, junto con diez de las entidades federativas en las que la conducta no es considerada un delito, por lo que la inexistencia de tipo facilita llevar a cabo esta conducta sin temer que sea sancionado penalmente*

Delito de suplantación de Identidad en Campeche

En el Estado de Campeche se adicionó un artículo 242 bis al Código Penal del Estado, mediante decreto 148 de la LXII Legislatura, publicado en P.O. 0435 de fecha 15 de mayo de 2017, mediante el cual se tipificó el delito de suplantación de identidad, quedando de la siguiente manera:

> ***ARTÍCULO 242 BIS.29 Comete el delito de suplantación de identidad quien se atribuya por cualquier medio la identidad de otra persona, u otorgue su consentimiento para llevarla a cabo, causando con***

ello, un daño o perjuicio obteniendo con ello un lucro indebido para sí o para otra persona. Este delito se sancionará con prisión de dos a cinco años y de doscientos a mil unidades de medida y actualización y en su caso la reparación del daño causado.

En el dictamen que dio origen a dicha reforma, el Congreso de Campeche reconoció la necesidad de establecer sanciones para las personas que se hagan pasar por otras o que otorguen su consentimiento para ello, utilizando indebidamente información personal. Esto incluye datos que se proporcionan a instituciones públicas, privadas y financieras, como bancos. Estas acciones pueden ser utilizadas para cometer delitos que dañan la integridad moral de las personas o afectan su patrimonio. Actualmente, estas conductas se evidencian en el uso de tecnología moderna en diversas operaciones y transacciones.

También se reconoció como bienes jurídicos tutelados la identidad de las personas y los datos que la componen como, el nombre y apellidos, el domicilio, la imagen, la nacionalidad, el registro de nacimiento, los rasgos físicos y las huellas dactilares, los cuales sirven para crear el perfil de una persona y que permiten establecer su identidad a diferencia de cualquier otra, y es precisamente el objetivo que persigue el delito de suplantación de identidad el cual consiste en hacerse pasar por otra persona para causar un daño u obtener un lucro indebido.

Por ello, el Congreso de Campeche estimó procedente adicionar el tipo penal con la finalidad de proteger la información que las personas físicas proporcionen a las diversas instituciones para que no se haga uso indebido de la misma ocasionándoles así una afectación a su integridad personal o su patrimonio.[8]

La suplantación de identidad y su relación con la Inteligencia Artificial

La inteligencia artificial se enfoca en crear sistemas y programas que pueden realizar tareas que requieren inteligencia humana, como el aprendizaje, la resolución de problemas y la toma de decisiones.

Es importante tener en cuenta que la Inteligencia Artificial actual, es muy buena en tareas específicas para las que ha sido programada por el humano, pero no posee una comprensión o conciencia general del mundo, carece de emociones, conciencia de sí misma, ni la capacidad de entender o aprender cualquier cosa fuera de su campo de entrenamiento específico, sistema implantado por el ser humano.

Es de nuestra incumbencia destacar que los 36 países que integran la *Organización para la Cooperación y el Desarrollo Económicos*, incluido México, firmaron, en mayo de 2019, un primer conjunto de directrices de políticas intergubernamentales en materia de inteligencia artificial.[9]

[8] Dictamen CÓDIGO PENAL CAMPECHE - Suplantación de Identidad (1).docx (congresocam.gob.mx)

[9] Recomendación sobre la inteligencia artificial, Instrumentos jurídicos de la OCDE. https://www.adigital.org/sin-categoria/la-ocde-publica-un-conjunto-de-directrices-y-recomendaciones-en-materia-de-inteligencia-artificial/

En tal sentido, la Organización para la Cooperación y el Desarrollo Económicos ha desarrollado un conjunto de principios para la Inteligencia Artificial. Estos principios se basan en cinco fundamentos:

1. *La Inteligencia Artificial debe beneficiar a las personas y al planeta impulsando el crecimiento inclusivo, el desarrollo sostenible y el bienestar.*

2. *Los sistemas de Inteligencia Artificial deben diseñarse respetando el estado de derecho, los derechos humanos, los valores democráticos y la diversidad.*

3. *Debe existir una transparencia y divulgación responsable en torno a los sistemas de Inteligencia Artificial, para garantizar que las personas entiendan sus resultados y puedan desafiarlos.*

4. *Los sistemas de Inteligencia Artificial deben funcionar de manera sólida y segura a lo largo de su ciclo de vida y los riesgos potenciales deben evaluarse y gestionarse continuamente.*

5. *Las partes interesadas deben colaborar para maximizar los beneficios de la Inteligencia Artificial y minimizar sus riesgos.*

La Inteligencia Artificial es sin duda alguna, una herramienta tecnológica que evolucionan rápidamente hacia una especie propia de pensamiento, de momento puede aportar grandes beneficios para la humanidad en áreas como la salud, ciencia, arte, educación y el esparcimiento.

Sin embargo, hay preocupaciones y cuestionamientos, incluso advertencias entre la comunidad dedicada al desarrollo de esta tecnología, sobre los riesgos que conllevan la Inteligencia Artificial, que puede violentar la dignidad humana o la propia seguridad de la sociedad, por lo que consideramos es necesario que se regule y se elaboren leyes que puedan garantizar el bienestar de las personas en una nueva realidad.

También es de destacar que el 22 de septiembre de 2024, la Asamblea General de la ONU adoptó el llamado Pacto para el Futuro, con el que el grupo de naciones pretende hacer frente los desafíos del siglo XXI.

En ese marco, los jefes de Estado y de Gobierno se comprometieron a llevar a cabo un total de 57 acciones para lograr hacer realidad sus intenciones. Tales acciones se dividen en diferentes áreas que van desde el impulso al desarrollo sostenible hasta poner a los jóvenes en el centro del cambio, pasando por los derechos humanos, la ciencia y sus interrelaciones. Las cinco grandes áreas de interés del Pacto son: desarrollo sostenible; paz y seguridad

internacionales; ciencia y tecnología; juventud y generaciones futuras y transformación de la gobernanza mundial.[10]

Uno de los objetivos fundamentales del Pacto para el Futuro es el de:

Mejorar la gobernanza internacional de la inteligencia artificial en beneficio de la humanidad

En tal sentido, una de las cuestiones más sobresalientes de la Cumbre fue uno de los acuerdos anexos al *Pacto del Futuro.*

Se trata del Pacto Mundial Digital, que es el primer acuerdo verdaderamente mundial sobre la regulación internacional de la inteligencia artificial (IA) y se basa en la idea de que la tecnología debe beneficiar a todos. Ese acuerdo esboza compromisos para garantizar que las tecnologías digitales contribuyan al desarrollo sostenible y a los derechos humanos, al tiempo que aborda riesgos como las brechas digitales, la ciberseguridad y el uso indebido de la tecnología.[11]

El Pacto pretende reducir la brecha digital y garantizar que las tecnologías de Inteligencia Artificial se utilicen de forma responsable, fomentando la cooperación mundial tanto en las capacidades de IA como en las amenazas a la seguridad. Los gobiernos también están comprometidos a formar un Panel Científico mundial imparcial, sobre Inteligencia Artificial y a iniciar una conversación internacional sobre la gobernanza de la IA en el seno de la ONU.

El problema urgente

Además de incorporar nuestras preocupaciones al entorno mundial y sumarnos activamente a los esfuerzos internacionales, es menester atender la problemática actual y urgente como lo son los fraudes y usurpación de identidad con la ayuda de la Inteligencia Artificial.

Falsificar identidades por medio de la Inteligencia Artificial es menos complejo de lo que se piensa. Está al alcance de cualquier persona. La utilización de la Inteligencia Artificial para la alteración de imágenes, audios o videos plantea una serie de riesgos y preocupaciones significativas en diferentes aspectos, ya que puede utilizarse para crear imágenes, videos, registros de voz falsos, que parecen auténticos, lo que plantea el riesgo de difundir información errónea o falsa, que puede vulnerar el derecho de las personas engañándolas para obtener un lucro. Esto puede tener graves consecuencias psicológicas para las víctimas.

La situación exige una respuesta integral que incluya no solo mejoras tecnológicas en los sistemas de seguridad, sino también la implementación de una legislación

[10] https://news.un.org/es/story/2024/09/1533016
[11] Ibidem

robusta que regule el uso de la Inteligencia Artificial para prevenir su explotación criminal.

Las leyes deben contemplar sanciones específicas para los delitos cometidos con el uso de Inteligencia Artificial y promover una mayor cooperación entre los sectores público y privado para desarrollar soluciones tecnológicas más seguras. Asimismo, la capacitación y concienciación de los ciudadanos sobre los riesgos de la IA y cómo protegerse contra estos nuevos tipos de fraude son esenciales para mitigar el impacto de la suplantación de identidad en el futuro digital.

Sin duda, tenemos que establecer un marco para abordar este tipo de situaciones y brindar protección a las víctimas. A medida que la inteligencia artificial avanza, se vuelve cada vez más difícil detectar la manipulación de imágenes, audios o videos. Esto puede dificultar la identificación de contenido falso o modificado.

Uno de los mayores riesgos que representa la IA en la suplantación de identidad es el uso de deepfakes, una tecnología que emplea aprendizaje profundo (deep learning) para crear videos, audios e imágenes falsificados pero altamente realistas.

Los delincuentes pueden crear videos o audios de ejecutivos, empleados o personas de confianza que ordenan transferencias de dinero o cambios en información confidencial, engañando a sus colegas y a las instituciones financieras. Este tipo de fraude es difícil de detectar y puede generar pérdidas significativas para las empresas y las víctimas individuales.

Por otro lado, los chatbots y los asistentes virtuales impulsados por IA son utilizados en fraudes de suplantación de identidad para interactuar con las víctimas de manera automatizada, emulando a representantes de instituciones bancarias, agencias gubernamentales o incluso amigos y familiares. Estas herramientas son capaces de sostener conversaciones fluidas y responder preguntas en tiempo real, lo que facilita que los delincuentes recopilen información personal o financiera de las víctimas.

Por ejemplo, un chatbot malicioso puede hacerse pasar por un empleado del banco y solicitar detalles de una cuenta, contraseñas o números de tarjetas de crédito.

Como ya comentamos, el phishing, una de las técnicas más comunes para suplantar identidad, ha sido potenciado por la IA. Tradicionalmente, los ataques de phishing eran masivos y poco personalizados, lo que facilitaba que las personas más atentas detectaran los fraudes. Sin embargo, con la IA, los delincuentes pueden crear campañas de phishing altamente personalizadas y dirigidas a objetivos específicos, mejorando significativamente la efectividad de sus ataques.

Mediante el uso de algoritmos de IA, los ciberdelincuentes pueden analizar grandes volúmenes de datos públicos sobre una persona (como redes sociales, correos electrónicos o información en línea) y diseñar correos electrónicos o mensajes de texto personalizados que imiten el estilo de comunicación de conocidos, colegas o

instituciones de confianza. Esta personalización hace que las víctimas confíen más en los mensajes y estén más propensas a compartir información confidencial o realizar acciones comprometedoras, como hacer clic en enlaces maliciosos o descargar archivos infectados.

La IA también facilita la creación de identidades falsas mediante la generación automática de perfiles en redes sociales, correos electrónicos o plataformas en línea que se asemejan a personas reales. Estas identidades falsas pueden ser utilizadas para engañar a personas, instituciones financieras o empresas, haciendo que el fraude de suplantación de identidad sea más difícil de detectar.

Los avances en la Inteligencia Artificial han permitido clonar con facilidad el rostro y la voz de cualquier persona, tan solo en México el robo de identidad con uso de IA incrementó 218% en el último año, ha indicado el Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México.[12]

El número de víctimas por robo de identidad a través de IA de enero a agosto ascendió a 1,607, cifra por arriba de 684 reportes que se recibieron el año pasado, los principales medios de obtención de información fueron a través de redes sociales y robo o hackeo de celular con 62.1 y 26.1% respectivamente.[13]

La Inteligencia Artificial está facilitando el trabajo a los ciberdelincuentes, éstos sólo necesitan archivos de voz para generar frases enteras; fotos o videos para crear circunstancias que afecten a las personas.

El fácil acceso a programas de Inteligencia Artificial, que pueden costar desde 200 pesos, permite que ciberdelincuentes puedan crear imágenes, videos y audios de las víctimas, con los que han logrado producir un daño patrimonial, en 90% de los casos entre 1,000 y 5,000 pesos, sin embargo, algunos son mayores a 50,000 pesos.[14]

Uno de los principales modos de operar es utilizando fotografías de redes sociales para alterarlas a fin de crear desde situaciones de infidelidad o sexuales y después amenazan a las víctimas con divulgar el contenido entre sus conocidos o venderlas como reales a través de sitios en Internet. Este esquema también ha sido encontrado en aplicaciones de los llamados monta deudas, las cuales hacen uso de la IA para extorsionar a las víctimas.

La Inteligencia Artificial también es utilizada para dar mayor credibilidad al fraude conocido como "La patrona", el cual consiste en crear una situación de emergencia entre empleado y empleador, en estos casos el trabajador recibe una llamada o mensajes de un número desconocido, el patrón indica que se encuentra en un percance y que necesita dinero, no obstante, la voz que se escucha en la llamada es un audio clonado y alterado a través de Inteligencia Artificial. Los ciberdelincuentes

[12] https://consejociudadanomx.org/contenido/suben-218-reportes-por-robo-de-identidad
[13] Ibidem
[14] Ibidem

usan la IA para el robo de datos personales y con ello tramitar tarjetas de crédito o utilizar las cuentas bancarias para compras que no son autorizadas.

La suplantación de identidad en el contexto de los fraudes cibernéticos es un problema creciente en México que requiere una respuesta legislativa contundente.

La protección de la identidad y los datos personales de los ciudadanos es un derecho fundamental que debe ser garantizado por el Estado. Asimismo, es esencial fortalecer la confianza en el ecosistema digital para impulsar el crecimiento económico y garantizar la seguridad en las transacciones en línea.

Para ello, es necesario contar con una legislación robusta, actualizada y coherente que aborde de manera integral la suplantación de identidad y que contemple tanto medidas preventivas como sanciones severas para los delincuentes. Solo así se podrá enfrentar de manera efectiva este tipo de delitos y proteger a las y los ciudadanos en el entorno digital.

Justificación jurídica de la propuesta

Como se ha mencionado con anterioridad, en la era digital surgen nuevas formas de cometer delitos, el uso de la inteligencia artificial no es ajena a esta situación y la suplantación de la identidad utilizando esta tecnología se está volviendo cada vez más común, de ahí la responsabilidad de las y los legisladores de presentar propuestas que den solución a este problema y sancionen a quienes pretenden violentar los derechos de las y los ciudadanos con el uso de nuevas tecnologías.

Para avanzar en este tema, es importante establecer **que previo a tipificar la suplantación de identidad por medio de la inteligencia artificial a nivel federal, se requiere en primera instancia tipificar el delito de suplantación de identidad,** ya que actualmente esa conducta delictiva solo se encuentra tipificada a nivel local.

Partiendo de lo anterior, la presente iniciativa propone incorporar un Capítulo IX, al Título Décimo Tercero, denominado "Falsedad", del Código Penal Federal. Se propone que la adición se realice en dicho apartado porque **en este título se encuentran tipificados los delitos relacionados con la alteración, simulación o modificación de la verdad para perjudicar a alguien.**

El Título Décimo Tercero actualmente contiene 8 capítulos en los que tipifica los delitos de: **1) falsificación, alteración y destrucción de moneda; 2) Falsificación y utilización indebida de títulos al portador, documentos de crédito público y documentos relativos al crédito; 3) Falsificación de sellos, llaves, cuños o troqueles, marcas, pesas y medidas; 4) Falsificación de documentos en general; 5) Falsedad en declaraciones judiciales y en informes dados a una autoridad; 6) Variación del nombre o del domicilio, 7) Usurpación de funciones públicas o de profesión y uso indebido de condecoraciones, uniformes, grados**

jerárquicos, divisas, insignias y siglas y 8) Disposiciones comunes a los capítulos precedentes.

Para establecer el tipo penal de suplantación de identidad se tomó como referencia el tipo penal previsto en el Estado de Campeche.

El tipo penal de suplantación de identidad propuesto considera los siguientes elementos:

- **Sujeto activo**: Cualquier persona, física o jurídica, que realice la suplantación. Es importante establecer que la suplantación de identidad no solo ocurre con personas físicas, si no puede ocurrir a personas jurídicas quienes también están expuestas a este tipo de conductas delictivas.
- **Sujeto pasivo**: La persona física o jurídica cuya identidad es suplantada.
- **Conducta**: Se comete el delito a quien se atribuya, apropie, transfiera o utilice la identidad de otro sin su consentimiento.
- **Finalidad**: El propósito de causar daño, perjuicio o lucro indebido es fundamental. Esto significa que la acción debe tener una intención maliciosa o fraudulenta.
- **Dolo:** La suplantación de identidad requiere dolo, es decir, la intención de realizar la acción sabiendo que es ilegal y que puede causar un daño.
- **Pena:** Este delito se sancionará con prisión de dos a cinco años y de doscientos a mil unidades de medida y actualización, y en su caso, la reparación del daño causado.

Con la tipificación de este delito se busca tutelar el derecho de las y los mexicanos como el derecho a la identidad, el derecho a la intimidad, el derecho a la honra y reputación, el derecho a la propiedad, el derecho a la seguridad personal y el derecho a la protección jurídica. También se incorpora a la pena la obligación de sujeto activo de reparar el daño causado a las víctimas,

Por lo que corresponde al uso de la suplantación de identidad utilizando la inteligencia artificial, la presente iniciativa propone establecer que se considerará equiparable al delito de suplantación de identidad, y se impondrán las mismas penas previstas en **este artículo a quien utilizando cualquier software o aplicación de inteligencia artificial, elabore, genere, distribuya o manipule imágenes, videos o audios con la intención de suplantar la identidad de una persona o hacer pasar dichos contenidos como reales.**

De esta forma, se **incorpora al tipo penal de suplantación de identidad como sujetos activos, a quienes utilicen software o aplicaciones de inteligencia artificial para cometer este delito. Además, se adicionan las siguientes conductas:**

- Elaborar: Crear contenidos desde cero.

- Generar: Producir imágenes, videos o audios.
- Distribuir: Compartir estos contenidos con otros.
- Manipular: Alterar contenidos existentes para cambiar su significado o autenticidad.

Se propone también establecer en la intencionalidad, la acción no solo de suplantar la identidad de una persona, sino también, al tratarse de inteligencia artificial, se debe prever la intención de hacer que los contenidos parezcan reales.

Finalmente, para brindar certeza jurídica al tipo penal se requiere definir qué es lo que se debe entender por software o aplicación de Inteligencia Artificial, para ello, tomamos como referencia la definición considerada por la Comisión Europa[15] que la *define como sistemas de software (y posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital:*

- *Percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados.*
- *Razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado.*
- *Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico. También pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas.*

Dicho de otro modo la inteligencia artificial (IA) es un campo de la informática que se enfoca en crear sistemas que puedan realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción. estos sistemas pueden percibir su entorno, razonar sobre el conocimiento, procesar la información derivada de los datos y tomar decisiones para lograr un objetivo dado.[16]

Considerando lo anterior, en la presente iniciativa se establece que **se debe entender por software de inteligencia artificial cualquier sistema, dispositivo o programa informático que posea la capacidad de realizar actividades que, tradicionalmente, requieren de la inteligencia humana para su ejecución, incluyendo, entre otros, sistemas de procesamiento de lenguaje natural, aprendizaje automático, redes neuronales y algoritmos avanzados.**

Por todo lo anteriormente examinado, es que someto a la consideración de esta Soberanía, la aprobación del siguiente proyecto de:

[15] Qué es la Inteligencia Artificial | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (planderecuperacion.gob.es)
[16] Qué es la Inteligencia Artificial | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (planderecuperacion.gob.es)

DECRETO POR EL QUE SE ADICIONA UN CAPÍTULO IX, AL TÍTULO DÉCIMO TERCERO, INCORPORANDO UN ARTICULO 252 BIS, AL CÓDIGO PENAL FEDERAL.

Artículo único. Se adiciona un Capítulo IX, al Título Décimo Tercero, incorporando un artículo 252 bis, al Código Penal Federal, para quedar como sigue:

CAPITULO IX
Suplantación de identidad

Artículo 252 Bis. - Comete el delito de suplantación de identidad quien, sin consentimiento de la persona física o jurídica, se atribuya, apropie, transfiera o utilice la identidad de otro, con el fin de causar un daño, perjuicio o de obtener un lucro indebido, propio o para un tercero.

Este delito se sancionará con prisión de dos a cinco años y de doscientos a mil unidades de medida y actualización, y en su caso, la reparación del daño causado.

Se considerarán equiparables al delito de suplantación de identidad, y se impondrán las mismas penas previstas en este artículo a quien utilizando cualquier software o aplicación de inteligencia artificial, elabore, genere, distribuya o manipule imágenes, videos o audios con la intención de suplantar la identidad de una persona o hacer pasar dichos contenidos como reales.

Para efectos de este artículo, se entenderá por software de inteligencia artificial cualquier sistema, dispositivo o programa informático que posea la capacidad de realizar actividades que, tradicionalmente, requieren de la inteligencia humana para su ejecución, incluyendo, entre otros, sistemas de procesamiento de lenguaje natural, aprendizaje automático, redes neuronales y algoritmos avanzados.

TRANSITORIOS

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

Senado de la República, a 12 de marzo de 2025

Sen. Alejandro Moreno Cárdenas