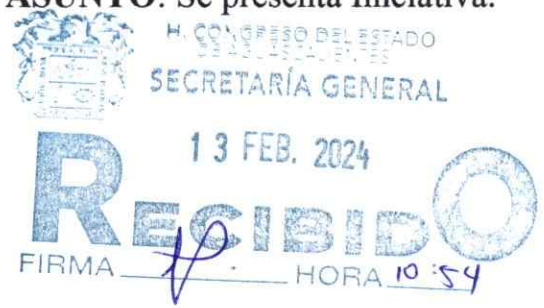




ASUNTO: Se presenta Iniciativa.



SEXAGÉSIMA QUINTA LEGISLATURA DEL HONORABLE CONGRESO DEL ESTADO DE AGUASCALIENTES PRESENTE.

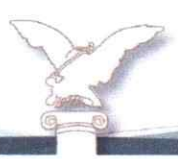
DIPUTADO ARTURO PIÑA ALVARADO, integrante del Grupo Parlamentario del Partido Movimiento de Regeneración Nacional de la Sexagésima Quinta Legislatura; con fundamento en los artículos 30, fracción I de la Constitución Política del Estado de Aguascalientes; 16, fracción III de la Ley Orgánica del Poder Legislativo del Estado de Aguascalientes; así como 153, de su propio Reglamento; someto ante la recta consideración de esta Honorable Asamblea, la ***“Iniciativa por la que se adiciona el artículo 181 C al Código Penal para el Estado de Aguascalientes”***, en materia del delito de usurpación de identidad de la persona al tenor de la siguiente:

E X P O S I C I Ó N D E M O T I V O S

La usurpación de identidad, entendida como el uso indebido de los datos personales y biométricos de una persona sin su autorización, se ha convertido en un delito cada vez más frecuente y preocupante en la era digital.

La identidad de la persona está formada por sus datos personales como: nombre, fecha de nacimiento, domicilio, fotografía, entre otros, es decir, cualquier dato que identifique a una persona.

Es importante señalar que la identidad es considerada un derecho humano, reconocido universalmente y perceptible a través de medios de identificación, es decir, principalmente datos, documentos y procedimientos. El derecho de identidad consiste en el reconocimiento jurídico y social de una persona como sujeto de derechos y responsabilidades y, a su vez,



de la pertenencia a un Estado, un territorio, una sociedad y una familia, condición necesaria para preservar la dignidad individual y colectiva de las personas.

Es por ello que la identidad, como derecho humano, está previsto y tutelado a nivel internacional. La Declaración Universal de Derechos Humanos, en su Artículo 6 protege el derecho a la identidad al establecer que todo ser humano tiene derecho, en todas partes al reconocimiento de su personalidad jurídica.

En el mismo sentido, el Pacto Internacional de Derechos Civiles y Políticos, en su Artículo 16 consagra: “todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica”, es decir que la ley debe de reconocer, garantizar y proporcionar los medios adecuados para que se otorgue esta personalidad.

A nivel nacional el derecho a la identidad está consagrado en nuestra ley fundamental como un derecho humano. Es importante mencionar que el 17 de junio de 2014 en la Constitución Política de los Estados Unidos Mexicanos, mediante Decreto, se adicionó al Artículo 4 la identidad como derecho humano, al establecer que toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento, resaltando en el propio Artículo la obligación del Estado de garantizarlo, lo que debe de efectuarse mediante la prevención, investigación, sanción y reparación a las violaciones del mismo, razón por la que debe ser tutelado, protegido y garantizado.

En otro orden de ideas, varios Tratados e Instrumentos Internacionales abordan la protección de datos personales y la prevención de la usurpación de identidad, por ejemplo Las Naciones Unidas (ONU) en su Declaración Universal de Derechos Humanos, en su Artículo 12, establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

También, el Convenio del Consejo de Europa sobre Protección de Datos Personales, establece principios para la protección de los datos personales y la privacidad, reconociendo la importancia de salvaguardar la información personal de los individuos.

La Directiva de Protección de Datos de la Unión Europea, establece normas para el procesamiento de datos personales dentro de la Unión Europea, incluyendo disposiciones sobre seguridad de datos y notificación de violaciones de seguridad.

Además, la Convención de Budapest sobre Ciberdelitos, aborda una amplia gama de delitos cibernéticos, incluida la usurpación de identidad, y promueve la cooperación internacional en la lucha contra el crimen en línea.

En México, la protección de datos personales y la prevención de la usurpación de identidad están reguladas por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Estas leyes establecen los derechos de los individuos sobre sus datos personales y las obligaciones de las organizaciones en su manejo y protección.

Asimismo, el Código Penal Federal tipifica la usurpación de identidad como un delito, estableciendo sanciones para quienes cometan este tipo de acciones fraudulentas. Fue reformado el 29 de junio de 2010, para crear el Capítulo III denominado de la “usurpación de identidad o personalidad” del Título XII, mediante el cual se adiciono el artículo 211 bis.

En el país, se ha tenido desarrollo normativo en la materia, en una primera instancia con la entrada en vigor de las leyes de transparencia, por ejemplo, el primer instrumento normativo en materia de protección de datos personales es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada el 11 de julio de 2002 en el Diario Oficial de la Federación que contempla apartados específicos en materia de protección de datos personales en el sector público.





Años después se publicó una reforma al artículo 6° constitucional, el 20 de julio del 2007, que incorpora el término “datos personales”, que fue más que nada en contexto con algunas reformas en materia de transparencia gubernamental, el cual establece lo siguiente:

“Artículo 6°

...El derecho a la información será garantizado por el Estado. Para el ejercicio del derecho de acceso a la información [...] en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.”

La Ley Federal de Transparencia y Acceso a la Información Gubernamental, publicada en el 2002, en un primer momento consideró a la protección de datos personales como un elemento del derecho de acceso a la información, al limitar la divulgación de información pública y solo permitir que las personas pudieran acceder y rectificar su información personal en posesión de autoridades.

Datos Personales en Posesión de los Particulares se encomendó al entonces Instituto Federal de Acceso a la Información y Protección de Datos, el carácter de autoridad garante de este derecho.

En 2014, todos los Institutos de Transparencia pasaron a ser órganos constitucionales autónomos y, en esta condición, se les atribuyó la responsabilidad de garantizar el derecho a la protección de datos personales.



Es de considerar que existe muy poco avance respecto al tema de Robo de Identidad, en la actualidad solo se ha reformado sobre el tema de la Protección de Datos Personales, lo cual se vio reflejado el 04 de mayo de 2015, con el decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública, así como con la creación de instituciones que regulan la Protección de datos como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales que es un organismo encargado fundamentalmente de garantizar el derecho de acceso de las personas a la información pública gubernamental, proteger los datos personales que están en manos tanto del gobierno federal, como de los particulares y resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.

Después, con la entrada en vigor la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que en 2016 se establecen un conjunto de obligaciones específicas a cargo de todas las autoridades para cumplir principios y deberes en la materia, y para garantizar los derechos de acceso, rectificación, cancelación y oposición, mejor conocidos por su acrónimo ARCO.

De esta manera, el derecho a la protección de datos personales es reconocido como un derecho independiente del derecho de acceso a la información pública.

Ahora bien, la usurpación de identidad, también conocida como suplantación de identidad, se refiere al acto de utilizar la información personal de otra persona, como su nombre, número de identificación, dirección, información biométrica, entre otros, con el fin de cometer fraudes, realizar transacciones ilegales o causar perjuicio a la víctima.

El fraude de identidad es un tipo de fraude en el que se roba la información personal de una persona y se utiliza ilegalmente para obtener beneficios personales.

En biometría, el fraude de identidad se refiere al uso engañoso o manipulación de los rasgos biológicos únicos de una persona, como las huellas dactilares o el reconocimiento



facial, para obtener acceso no autorizado o llevar a cabo actividades fraudulentas. Implica utilizar los datos biométricos para hacerse pasar por la persona legítima y engañar a los sistemas de autenticación biométrica.

Los datos biométricos, como las huellas dactilares, el reconocimiento facial o los escaneos del iris, se consideran muy personales y difíciles de replicar, lo que los convierte en un objetivo valioso para los estafadores.

Es entonces que el fraude de identidad ocurre cuando un impostor obtiene acceso no autorizado a los datos biométricos de alguien y los utiliza para engañar a los sistemas de autenticación biométrica.

Lo anterior se puede lograr mediante métodos como huellas dactilares falsificadas, apariencias faciales falsas o patrones de iris modificados para hacerse pasar por el individuo legítimo. Al falsificar sus rasgos biométricos, los estafadores pueden acceder de manera fraudulenta a sistemas seguros, eludir los procesos de verificación de identidad o realizar transacciones no autorizadas.

Las consecuencias del fraude de identidad biométrica pueden ser graves, pues una vez que un impostor obtiene acceso a los datos biométricos de una persona, es difícil recuperar o proteger ese identificador comprometido.

Las personas afectadas podrían sufrir brechas de seguridad, pérdidas económicas y la posible exposición de su información personal. Proteger los datos biométricos, implementar medidas de seguridad sólidas y monitorizar continuamente las actividades sospechosas son acciones cruciales para reducir los riesgos de fraude de identidad en el contexto biométrico.

También se tiene que el robo de identidad es la práctica ilícita de robar o manipular las características biológicas únicas de una persona, como las huellas dactilares o los rasgos faciales, para asumir de manera fraudulenta su identidad.



Bajo el mismo sentido, el robo de identidad implica la adquisición no autorizada y el uso fraudulento de datos biométricos para engañar a los sistemas de autenticación biométrica y obtener acceso a sistemas seguros o realizar actividades ilícitas en nombre de la víctima.

Si bien, el fraude de identidad y el robo de identidad son conceptos estrechamente relacionados, pero con claras diferencias, ya que el robo de identidad consiste en adquirir y utilizar, de forma no autorizada, la información personal de alguien.

Por lo general, implica el robo de información personal, como el número de la Seguridad Social, datos de tarjetas de crédito o información de cuentas bancarias.

Por otro lado, el fraude de identidad se refiere al uso engañoso o manipulación de la información personal de una persona, incluidos los datos biométricos, para obtener acceso no autorizado o realizar actividades fraudulentas, o sea, implica aprovechar los identificadores personales para engañar a los sistemas de autenticación.

Un ejemplo real de fraude de identidad podría ser cuando alguien utiliza la huella dactilar o el reconocimiento facial de otra persona para eludir las medidas de seguridad y obtener acceso a sus dispositivos personales, cuentas bancarias u otros sistemas protegidos.

En resumen, mientras que el fraude de identidad se centra en la manipulación o el engaño de datos biométricos o identificadores personales, el robo de identidad gira en torno a la adquisición y uso indebido de información personal para actividades fraudulentas.

Existen varias maneras en las que se puede presentar el fraude de identidad digital, como los correos electrónicos de suplantación de identidad, las estafas en las redes sociales y los sitios web falsos diseñados para engañar a las personas y hacer que revelen su información personal o financiera.



Este tipo de fraude representa una amenaza significativa en el mundo en línea actual y los métodos de autenticación tradicionales pueden no ser siempre suficientes para proteger la información personal de las personas. Esta es la razón por la que la tecnología biométrica, que utiliza las características físicas o de comportamiento únicas de una persona para la autenticación, se está convirtiendo en un aspecto cada vez más vital de la protección de la identidad digital.

El fraude de identidad es un delito complejo y en evolución que puede ocurrir a través de diferentes métodos y canales. Entender cómo ocurre el fraude de identidad puede ayudar a las personas y organizaciones a protegerse mejor contra esta amenaza tan frecuente.

A continuación se muestran algunas de las formas clave en las que ocurre el fraude de identidad:

- Suplantación de identidad: Los delincuentes cibernéticos utilizan correos electrónicos, mensajes de texto o llamadas telefónicas engañosas para hacer que las personas revelen su información personal. Estos intentos de suplantación de identidad a menudo se hacen pasar por entidades legítimas, como bancos o agencias gubernamentales, y solicitan a las víctimas que proporcionen detalles confidenciales como números de cuenta o contraseñas.
- Violación de los datos personales: Las violaciones de datos personales a gran escala exponen información personal en poder de las organizaciones. Los estafadores se aprovechan de estas brechas obteniendo los datos expuestos y utilizándolos para suplantar la identidad de personas o realizar transacciones fraudulentas.
- Ingeniería social: Esta técnica consiste en manipular a las personas para que divulguen voluntariamente información sensible. Los estafadores pueden hacerse pasar por autoridades o utilizar tácticas psicológicas para ganarse la confianza de sus objetivos y convencerlos de que compartan datos personales.
- Fraude de identidad sintética: Los estafadores crean identidades falsificadas combinando información real e inventada. Utilizan estas identidades sintéticas para



establecer un historial crediticio, abrir cuentas y obtener préstamos, lo que a menudo deja a las instituciones financieras con pérdidas significativas.

- **Skimming:** Los delincuentes utilizan skimmers para capturar la información de la tarjeta de crédito o débito cuando la persona utiliza el cajero automático o hace una compra. Estos datos robados luego se utilizan para crear tarjetas falsificadas o realizar transacciones no autorizadas.
- **Apropiación fraudulenta de cuenta:** Los estafadores obtienen acceso no autorizado a cuentas bancarias, cuentas de tarjetas de crédito o perfiles en línea de personas mediante la explotación de contraseñas débiles, ingeniería social u otras técnicas de piratería. Una vez que tienen el control, pueden llevar a cabo transacciones fraudulentas o aprovechar la cuenta comprometida en su propio beneficio. Para protegerse contra el fraude de identidad, los particulares y las organizaciones deben emplear prácticas de seguridad sólidas como utilizar contraseñas únicas y complejas, habilitar la autenticación multifactor, supervisar regularmente las cuentas financieras en busca de actividad inusual y permanecer atentos a los intentos de suplantación de identidad y a las comunicaciones sospechosas. Además, el uso de tecnologías avanzadas como la biometría puede mejorar la verificación de la identidad y proporcionar una capa adicional de seguridad al validar los rasgos físicos o de comportamiento únicos de un individuo.

No cabe duda que el fraude de identidad es una amenaza creciente que puede tener diversas consecuencias más allá de las pérdidas financieras. Para detectar y prevenir esta práctica, es imprescindible permanecer alerta en todos los aspectos de nuestra vida diaria.

Es claro que la tecnología biométrica presenta una solución prometedora para combatir y gestionar el fraude de identidad de forma eficaz. Al utilizar nuestras características físicas únicas, como huellas dactilares, reconocimiento facial e incluso escaneos del iris, la biometría proporciona un método altamente seguro de verificación de identidad que es difícil de falsificar, pero que también se puede ser corrompida.



Los datos estadísticos sobre usurpación de identidad son difíciles de recopilar de manera precisa debido a la naturaleza subestimada del delito y la falta de denuncias. Sin embargo, según la Comisión Federal de Comercio de los Estados Unidos, se estima que millones de personas son víctimas de usurpación de identidad cada año a nivel mundial, con costos económicos significativos y repercusiones emocionales para las víctimas.

En México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) reporta un aumento en los casos de fraude y usurpación de identidad, especialmente en el ámbito de las transacciones financieras en línea y el robo de información personal.

El robo de identidad es un delito que en los últimos años ha crecido de forma exponencial, afectando no sólo a usuarios sino también la reputación de las empresas y es que el organismo aserró que el número de reclamaciones por este delito creció durante la pandemia un promedio de 11%. En el año 2011 se atendieron 4,000 quejas por presunto robo de identidad, mientras que en 2015 las cifras se elevaron a 10,000.

Nuestro país ocupa el octavo lugar en suplantación de identidad. Tan solo de enero a septiembre de 2021, se registraron 4,453,043 reclamaciones en el sector bancario.

Asimismo, se estima que 9 de cada 10 personas llevan información suficiente en su cartera para ser víctima de robo de identidad según cifras de CPP México, el 86% lleva en su cartera la credencial para votar, el 49% la tarjeta de débito, el 30% la licencia de conducir, 27% tarjetas departamentales y 17% tarjetas de crédito.

De acuerdo con datos del Banco de México y firmas especializadas, México ocupa el 8º lugar en este delito en el mundo y el 2º lugar en América Latina, 67% es por pérdida de documentos, 63% por robo de una cartera y portafolios y 53% es información tomada de una tarjeta bancaria.



La delincuencia poco a poco ha ido perfeccionando esta actividad delictiva, a través de técnicas, conocimientos y artimañas, como la clonación de documentos por ejemplo la credencial para votar, pasaporte, actas de nacimientos, etc., con el único propósito de suplantar la identidad de las personas para poder contratar servicios y/o productos en su nombre.

Adicional a las pérdidas económicas del ciudadano, también las instituciones pierden anualmente millones de pesos por esta actividad, de la cual nadie tiene la culpa y al final no hay responsables.

De acuerdo al estudio elaborado por la Comisión Nacional para la Protección y Defensa de Servicios Financieros a partir de información de la Comisión Nacional Bancaria y de Valores, y con base a las reclamaciones con impacto monetario señalan que en 2015, el monto reclamado por los usuarios ascendió a 708 millones de pesos.

En la gráfica se describen los montos de las reclamaciones con impacto monetario de los años 2011 al 2015, así como también incluye el tercer trimestre de 2016:



La población que utiliza internet también va en aumento, el Instituto Nacional de Estadística y Geografía (INEGI), la Secretaría de Comunicaciones y Transportes (SCT) y el Instituto Federal de Telecomunicaciones, elaboran anualmente la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), la cual revela que en México hay 80.6 millones de usuarios de Internet, que representan el 70.1% de la población de seis años o más.

Esta cifra revela un aumento de 4.3 puntos porcentuales respecto de la registrada en 2018 (65.8%) y de 12.7 puntos porcentuales respecto a 2015 (57.4 %), este aumento sostenido implica un gran reto para el derecho a la identidad.

Es en cuanto que la usurpación de identidad representa una amenaza seria para la privacidad y seguridad de las personas en la era digital. La protección de datos personales y biométricos, la implementación de medidas de seguridad cibernética y la concienciación pública son fundamentales para prevenir este tipo de delitos y proteger los derechos individuales.

En un mundo cada vez más interconectado, es crucial que los gobiernos, las organizaciones y los individuos trabajen juntos para salvaguardar la identidad y privacidad de las personas.

Es por ello que el derecho a la identidad debe de ser garantizado por el Estado y una de las formas de hacerlo es a través de la política criminal y el establecimiento de leyes, mismas que deben ser claras.

Por lo tanto, la presente iniciativa tiene como finalidad incorporar en el Código Penal del Estado de Aguascalientes el tipo penal de usurpación de identidad, entendido este, cuando una o más personas simulen, elaboren, alteren, manipulen, obtengan, transfieren, utilicen o se apropien de manera indebida, de los datos personales y biométricos de otra sin la autorización de ésta última.



Al que indebidamente por cualquier medio usurpe la identidad de cualquier persona o, con fines de lucro o delictuosos, será sancionado con una pena de prisión de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa. Asimismo, preveer el aumento de pena en el caso de que la víctima sea una persona menor de dieciocho años de edad o que no tiene la capacidad para comprender el significado del hecho o que no tiene la capacidad para resistirlo.

Por lo que es trascendente considerar la legalidad, al establecer la norma protectora de los bienes jurídicos más preciados de toda sociedad en este caso la identidad, toda vez que no hay delito sin ley y no hay pena sin ley, y las lamentables consecuencias que se gestan, como se ha podido observar en la presente inciativa, afectan directamente al individuo.

Asimismo, es menester tomar en cuenta la lesivilidad del bien jurídico, lo que cause daño a otro, ello se refleja en los índices de “usurpación de identidad” que se presentan en diversos ámbitos. De igual forma, resaltar relevante la proporcionalidad de la sanción, considerando la gravedad del delito.

Como es cierto, la tecnología se ha convertido en una herramienta esencial, sin embargo, la delincuencia también ha usado estas herramientas para aprovecharse de los ciudadanos y el robo de identidad se ha convertido en una de las amenazas más comunes. Con el uso de softwares, los delincuentes pueden obtener información personal, correos y hackear a organismos gubernamentales para suplantar identidades para cometer diversos delitos.

Por lo que, es necesario fortalecer y darle un enfoque preventivo a la política criminal del Estado mexicano, a efecto de proteger los datos personales de toda la población, toda vez que ponen en riesgo la seguridad, integridad y patrimonio de las personas, así como el de sus familias.



Para mantener a la población alerta respecto al delito de robo de identidad, también es recomendable que se realicen campañas informativas para prevenir que sean víctimas del delito en comento, otorgándoles información acerca de este tema, así como las medidas de prevención que tienen que tener las personas para evitar ser víctima de este delito y dando información después de ser saber que ya son víctimas del delito de robo de identidad.

Sin duda, la incorporación del delito de usurpación de identidad en el Código Penal de Aguascalientes se presenta como una medida esencial y oportuna en la era digital en la que vivimos.

La protección de la identidad y los datos personales de los ciudadanos no solo es una necesidad imperante para garantizar su seguridad y privacidad, sino que también constituye un pilar fundamental para mantener la confianza en los sistemas gubernamentales, financieros y sociales.

La inclusión de esta disposición legal no solo enviará un mensaje claro sobre la gravedad de las acciones fraudulentas relacionadas con la manipulación indebida de información personal y biométrica, sino que también proporcionará a las autoridades las herramientas necesarias para investigar y sancionar de manera efectiva a quienes cometan tales actos ilícitos.

En última instancia, esta medida fortalecerá el marco jurídico y contribuirá a preservar la integridad y dignidad de los ciudadanos de Aguascalientes en un entorno digital cada vez más complejo y susceptible a los abusos.

Para mejor ilustración de la reforma que se propone, a continuación, se presenta el siguiente cuadro comparativo:



CÓDIGO PENAL PARA EL ESTADO DE AGUASCALIENTES

TEXTO VIGENTE	TEXTO PROPUESTO
Sin correlativo.	<p>ARTÍCULO 181 C.- Usurpación de Identidad. Se entiende por usurpación de identidad cuando una o más personas simulen, elaboren, alteren, manipulen, obtengan, transfieren, utilicen o se apropien de manera indebida, de los datos personales y biométricos de otra persona sin la autorización de ésta última.</p> <p>Al que indebidamente por cualquier medio usurpe la identidad de cualquier persona o, con fines de lucro o delictuosos, será sancionado con una pena de prisión de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.</p> <p>Se aumentarán las sanciones previstas en el párrafo anterior hasta una tercera parte cuando la víctima sea una persona menor de dieciocho años de edad o que no tiene la capacidad para comprender el significado del hecho o que no tiene la capacidad para resistirlo.</p> <p>Además, se aumentarán las sanciones previstas en el párrafo segundo hasta una mitad en su mínimo y máximo, cuando:</p> <p>I. Se valga de la homonimia, parecido físico o similitud de la voz para la comisión del delito.</p>



	<p>II. Cuando se auxilie con medios y herramientas tecnológicas tales como software o aplicaciones que cuenten con inteligencia artificial.</p> <p>III. Manipule fotografías, videos o audios de la víctima.</p> <p>Tratándose de servidores públicos que, en ejercicio de sus funciones o aprovechando su cargo, permita, auxilie, autorice o tolere cualesquiera de las conductas señaladas en este artículo, además de ser sancionados por las mismas penas previstas en el presente artículo, será destituido e inhabilitado de dos a cinco años para desempeñar otro empleo, cargo o comisión públicos.</p>
--	---

Por lo anteriormente expuesto y fundado someto ante la recta consideración del Pleno Legislativo el siguiente:

PROYECTO DE DECRETO

ARTÍCULO ÚNICO. – Se adiciona el artículo 181 C al *Código Penal para el Estado de Aguascalientes*, para quedar como sigue:

ARTÍCULO 181 C.- Usurpación de Identidad. Se entiende por usurpación de identidad cuando una o más personas simulen, elaboren, alteren, manipulen, obtengan,



transfieren, utilicen o se apropien de manera indebida, de los datos personales y biométricos de otra persona sin la autorización de ésta última.

Al que indebidamente por cualquier medio usurpe la identidad de cualquier persona o, con fines de lucro o delictuosos, será sancionado con una pena de prisión de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.

Se aumentarán las sanciones previstas en el párrafo anterior hasta una tercera parte cuando la víctima sea una persona menor de dieciocho años de edad o que no tiene la capacidad para comprender el significado del hecho o que no tiene la capacidad para resistirlo.

Además, se aumentarán las sanciones previstas en el párrafo segundo hasta una mitad en su mínimo y máximo, cuando:

I. Se valga de la homonimia, parecido físico o similitud de la voz para la comisión del delito.

II. Cuando se auxilie con medios y herramientas tecnológicas tales como software o aplicaciones que cuenten con inteligencia artificial.

III. Manipule fotografías, videos o audios de la víctima.

Tratándose de servidores públicos que, en ejercicio de sus funciones o aprovechando su cargo, permita, auxilie, autorice o tolere cualesquiera de las conductas señaladas en este artículo, además de ser sancionados por las mismas penas previstas en el presente artículo, será destituido e inhabilitado de dos a cinco años para desempeñar otro empleo, cargo o comisión públicos.



ARTÍCULO TRANSITORIO

ÚNICO. – El presente Decreto iniciará su vigencia al día siguiente al de su publicación en el Periódico Oficial del Estado.

Palacio Legislativo de la Ciudad de Aguascalientes,
a los nueve días del mes de febrero del año 2024.

A T E N T A M E N T E



DIPUTADO ARTURO PIÑA ALVARADO

