# Universidad Tecnológica Ecotec
# Facultad De Derecho Y Gobernabilidad

## Título:

"Análisis Jurídico del Delito de Suplantación de Identidad por el Uso de Inteligencia Artificial en el Ecuador"

## Línea de investigación:

Gestión De Relaciones Jurídicas

## Modalidad de titulación:

Virtual

## Carrera:

Derecho con énfasis en Ciencias Penales y Criminológicas

## Titulo a obtener:

Trabajo de Titulación Previo a la Obtención del Título de Abogada de los Tribunales y Juzgados de la República del Ecuador


## Autoras:

Karla Nohemi Cedeño Torres
Julissa Elena Ruiz Ruiz

## Tutor:

Mgtr. Miguel Emilio Félix Romero


**Samborondón - Ecuador**

**2024**

***ANEXO No. 9***

PROCESO DE TITULACIÓN
***CERTIFICADO DE APROBACIÓN DEL TUTOR***

Samborondón, 08 de Agosto de 2024

Magíster o Doctor
**AB. ANDRES MADERO POVEDA**
**Unidad Académica: Facultad de Derecho**
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO**:** **"ANÁLISIS JURÍDICO DEL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR EL USO DE INTELIGENCIA ARTIFICIAL EN EL ECUADOR"**, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: **Cedeño Torres Karla Nohemí y Ruiz Ruiz Julissa Elena,** para que proceda con la presentación oral del mismo.

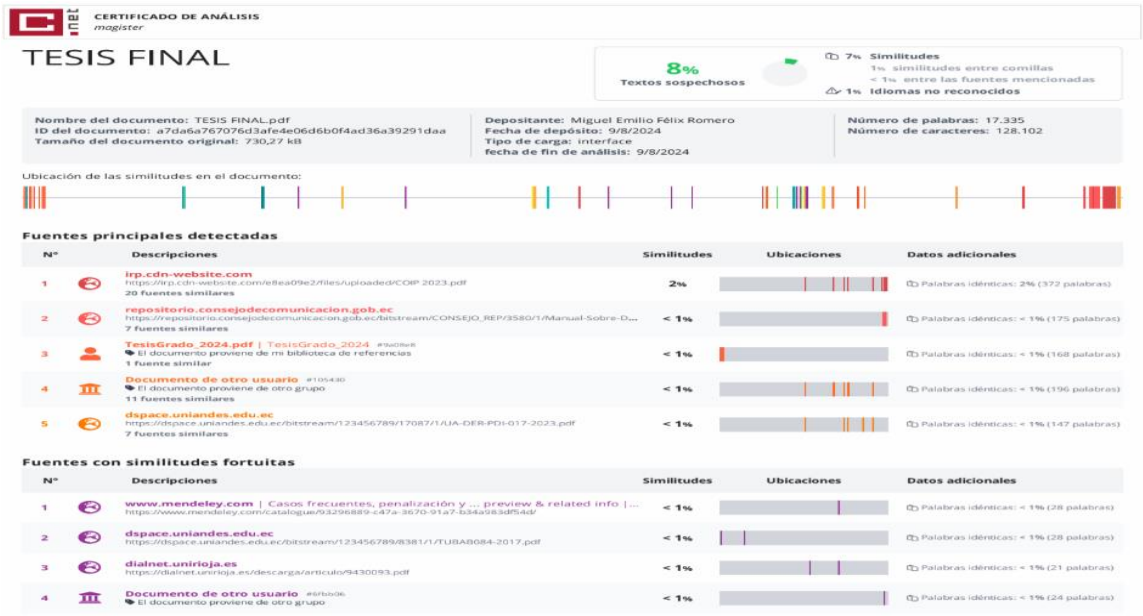
**ATENTAMENTE,**


**Firma**
**Mgtr. MIGUEL EMILIO FELIX ROMERO**
**Tutor(a)**

## ANEXO No. 10

***PROCESO DE TITULACIÓN***
***CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS***
***DEL TRABAJO DE TITULACIÓN***

Habiendo sido revisado el trabajo de titulación TITULADO: **"ANÁLISIS JURÍDICO DEL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR EL USO DE INTELIGENCIA ARTIFICIAL EN EL ECUADOR"** elaborado por **Cedeño Torres Karla Nohemí y Ruiz Ruiz Julissa Elena** fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del (%) **8** mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.



CERTIFICADO DE ANÁLISIS
magister

TESIS FINAL

8% Textos sospechosos

7% Similitudes
1% similitudes entre comillas
< 1% entre las fuentes mencionadas
1% Idiomas no reconocidos

Nombre del documento: TESIS FINAL.pdf
ID del documento: a7da6a767076d3afe4e06d6b0f4ad36a39291daa
Tamaño del documento original: 730,27 kB

Depositante: Miguel Emilio Félix Romero
Fecha de depósito: 9/8/2024
Tipo de carga: interface
fecha de fin de análisis: 9/8/2024

Número de palabras: 17.335
Número de caracteres: 128.102

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | irp.cdn-website.com<br>https://irp.cdn-website.com/e8ea09e2/files/uploaded/COIP 2023.pdf<br>20 fuentes similares | 2% | | Palabras idénticas: 2% (372 palabras) |
| 2 | repositorio.consejodecomunicacion.gob.ec<br>https://repositorio.consejodecomunicacion.gob.ec/bitstream/CONSEJO_REP/3580/1/Manual-Sobre-D...<br>7 fuentes similares | < 1% | | Palabras idénticas: < 1% (175 palabras) |
| 3 | TesisGrado_2024.pdf \| TesisGrado_2024<br>El documento proviene de mi biblioteca de referencias<br>1 fuente similar | < 1% | | Palabras idénticas: < 1% (168 palabras) |
| 4 | Documento de otro usuario<br>El documento proviene de otro grupo<br>11 fuentes similares | < 1% | | Palabras idénticas: < 1% (196 palabras) |
| 5 | dspace.uniandes.edu.ec<br>https://dspace.uniandes.edu.ec/bitstream/123456789/17087/1/UIA-DER-PDI-017-2023.pdf<br>7 fuentes similares | < 1% | | Palabras idénticas: < 1% (147 palabras) |

Fuentes con similitudes fortuitas

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | www.mendeley.com \| Casos frecuentes, penalización y ... preview & related info \| ...<br>https://www.mendeley.com/catalogue/93296889-c47a-3670-91a7-b34a983df54d/ | < 1% | | Palabras idénticas: < 1% (28 palabras) |
| 2 | dspace.uniandes.edu.ec<br>https://dspace.uniandes.edu.ec/bitstream/123456789/8381/1/TUBA8084-2017.pdf | < 1% | | Palabras idénticas: < 1% (28 palabras) |
| 3 | dialnet.unirioja.es<br>https://dialnet.unirioja.es/descarga/articulo/9430093.pdf | < 1% | | Palabras idénticas: < 1% (21 palabras) |
| 4 | Documento de otro usuario<br>El documento proviene de otro grupo | < 1% | | Palabras idénticas: < 1% (24 palabras) |

**ATENTAMENTE,**

Firmado electrónicamente por:
MIGUEL EMILIO FELIX ROMERO

**Firma**
**Mgtr/ PhD. MIGUEL EMILIO FELIX ROMERO**

**Tutor(a)**

## Agradecimientos

*Debo decir que durante este proceso existió altas y bajas, muchas veces nos queremos rendir y tirar la toalla inclusive no saber nada del tema ya sea porque nos parece difícil la tarea o pasamos por momentos donde no nos encontramos bien, sin embargo prevaleció el esfuerzo y la dedicación a este trabajo de investigación durante este tiempo para luego al finalizar este periodo obtener un resultado muy satisfactorio y es gracias a las personas que estuvieron a mi lado o que a la distancia me enviaban mensajes de apoyo y confianza, que me demostraron que los buenos amigos y la familia siempre están en los peores y también los buenos momentos. Quiero agradecer a todos ellos, nada de esto hubiera sido posible con el apoyo constante y las palabras de fuerza y ánimo de mis seres queridos cuando mas lo necesitaba.*

## Dedicatoria

*Dentro de este trabajo se encuentra el esfuerzo, la dedicación y el tiempo. Este trabajo refleja que una persona a pesar de no poder con todo, de no tener el conocimiento necesario, se puede arriesgar y ganar; si el ser humano se lo propone es capaz de lograr grandes cosas. He aquí una tarea más finalizada y la última dentro del largo proceso de la carrera. Es por eso, que mi dedicatoria va hacia mi misma, para demostrarme que, si se puede lograr todo, cualquier cosa inclusive la más difícil o las imposibles, que a veces solo es el miedo y la frustración jugando en nuestra cabeza pero que siempre se encuentra el camino, la salida y la solución.*

## Resumen

La finalidad de este trabajo de investigación es analizar minuciosamente la ley penal de nuestro ordenamiento jurídico respecto al delito de Suplantación de Identidad, ya que es uno de los delitos que se cometen con frecuencia en nuestro país y a su vez examinar como el uso progresivo de las diferentes tecnologías y uso especifico de la Inteligencia Artificial (IA) influye en el cometimiento de este delito, así mismo, estudiar los delitos informáticos que se encuentran relacionados a la suplantación de identidad con la contribución de la inteligencia artificial y en consecuencia otros tipos penales que se pueden generar o no a partir de esta conducta penal. La evolución de la tecnología influye demasiado en nuestra sociedad, y con esa evolución también surgen nuevas técnicas y formas para delinquir, por lo cual, dentro del ámbito penal se debe analizar estas conductas para su regulación. La norma penal debe reformarse constantemente para regular aquellas nuevas conductas que están apareciendo y que deben ser tipificadas dentro de la ley; el Derecho es cambiante, así como evoluciona la sociedad y la tecnología también lo hace el Derecho para cubrir las necesidades de los seres humanos.


***Palabras claves:*** Suplantación de Identidad, Inteligencia Artificial, Delitos Informáticos, Código Orgánico Integral Penal, Tecnología, Informáticos, Deepfake, Datos Personales.


## Abstract

The purpose of this research work is to thoroughly analyze the criminal law of our legal system regarding the crime of Identity Theft, since it is one of the crimes that are frequently committed in our country and at the same time examine how the progressive use of different technologies and specific use of Artificial Intelligence (AI) influences the commission of this crime, likewise, studying computer crimes that are related to identity theft with the contribution of artificial intelligence and consequently other types of crimes that They may or may not be generated from this criminal conduct. The evolution of technology greatly influences our society, and with this evolution new techniques and ways to commit crimes also arise, which is why, within the criminal field, these behaviors must be analyzed for their regulation. The criminal law must be constantly reformed to regulate those new behaviors that are appearing and that must be classified within the law; The Law is changing, just as society and technology evolve, so does the Law to meet the needs of human beings.


***Keywords:*** Identity Theft, Artificial Intelligence, Computer Crimes, Comprehensive Organic Criminal Code, Technology, Computer Scientists, Deepfake, Personal Data.

## Contenido

## 1. Introducción

El Ecuador como en otras partes del mundo ha evolucionado con la ayuda de la tecnología influyendo en muchos aspectos de la vida cotidiana. En los últimos tiempos también surge un aumento de delitos electrónicos en nuestro país, ya que los delincuentes encuentran en la tecnología nuevas formas para llevar a cabo un delito; estas personas tienen un gran conocimiento e intelecto respecto a la informática por lo cual se les hace fácil acceder a cualquier sistema informático traspasando cualquier tipo de seguridad.

A medida que se hacen mas frecuentes estos delitos quedan vulnerables los datos personales que se encuentran resguardados en bases de datos y expuestos en la red; datos personales que pueden ser utilizados, modificados y eliminados, en consecuencia, si no se le da un tratamiento correcto a los datos personales u otra información de importancia puede perjudicar a una o otra persona. Es el caso de los delitos de suplantación de identidad, normalmente la operación de este delito se basa en que en una persona utiliza datos personales de otra persona para sustituir su identidad consiguiendo un beneficio para si mismo o para un tercero, en concurrencia pasa cuando se hurtan cédulas de identidad, tarjetas de créditos, contraseñas y usuarios o cuando solicitan datos personales por medio de vía telefónica o mensajes de textos para así llevar a cabo su cometido.

Entonces, haciendo un enfoque en el ámbito penal, se observa que dentro de nuestra ley penal existe la necesidad de ampliar el contexto en cuanto al delito de la suplantación de identidad, debido a que con la gran influencia de la tecnología y también de la aparición de la Inteligencia Artificial, los ciberdelincuentes encuentran la forma para poder suplantar una identidad por medio de los sistemas informáticos creando perfiles más complejos y creíbles en las redes, haciendo mucho más fácil el trabajo de delinquir ya que, en cuestión de segundo lo pueden lograr por la rapidez de la red y también lo hace muy llamativo por su menudo precio.

Las autoridades competentes, expertos en la materia penal y de delitos informáticos deben concluir que el uso indebido de la tecnología y de la Inteligencia Artificial puede ayudar a la suplantación de identidad y al acceso indebido a los datos personales y sistemas. Es necesario analizar la ley penal vigente, así como las complementarias para encontrar las falencias y vacíos legales; y consecuentemente

establecer su reforma para convertirlas en más consistentes a la hora de enfrentar las nuevas conductas delictivas y simultáneamente dentro del contexto legal determinar niveles de responsabilidad para quienes estén involucrados en ejecutar el delito, para los que están al cuidado meticuloso de los datos personales y se presten para compartirlos sin la autorización del titular.

### 1.1. Antecedentes

En el Ecuador en los últimos años se han incrementado los delitos cibernéticos, siendo el más común, la suplantación de identidad por medios electrónicos, delito que ha tomado fuerza desde el 2016, con la aparición de las nuevas tecnologías, más específicamente la Inteligencia Artificial, se estima que este delito aumentará de forma significativa. Para el cometimiento de estos delitos, no se requiere grandes cantidades de dinero, al contrario, se hace atractivo por su bajo costo, y es catalogado como un delito transnacional, porque por lo general, el lugar de origen del ciberdelincuente, no suele ser el mismo que el de la víctima. En el código orgánico integral penal (COIP), encontramos tipificado este delito, en el artículo 212, que nos indica ‘‘La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años’’. Se analizará la eficacia y suficiencia que tiene este articulado con la presencia de la inteligencia artificial que cada día se hace más presente en la sociedad y la necesidad que tipificar su uso para el cometimiento de este delito, como agravante.

### 1.2. Planteamiento Del Problema

La necesidad actual en Ecuador de abordar el problema de “Analizar los delitos de suplantación de identidad y su potencial incremento utilizando inteligencia artificial” se debe a la creciente digitalización y los riesgos asociados al abuso de tecnología avanzada. Esto incluye preocupaciones sobre un posible aumento del robo de identidad mediante inteligencia artificial, lo que requiere una evaluación detallada de las leyes existentes y medidas apropiadas para proteger las identidades de los ciudadanos en el entorno digital. Para lograr un estado óptimo en el Ecuador en este tema, es necesario implementar una legislación sólida y actualizada que aborde específicamente temas relacionados con la inteligencia artificial y la protección de la identidad digital. Además, el gobierno, las agencias pertinentes y el sector privado

deben hacer un esfuerzo concertado para desarrollar y adoptar tecnologías de seguridad confiables, así como programas de concientización para informar al público sobre los riesgos involucrados y las medidas preventivas. La cooperación internacional también puede resultar beneficiosa para compartir mejores prácticas y enfoques eficaces para combatir la suplantación de identidad en el contexto de la IA. El uso específico de la IA para cometer delitos de suplantación de identidad aún está en sus inicios, pero crece la preocupación sobre su potencial. La tecnología de inteligencia artificial se puede utilizar para crear perfiles más detallados de personas a partir de datos disponibles en Internet, lo que facilita la creación de identidades falsas más complejas. Esto podría incluir la creación de perfiles falsos en las redes sociales, la creación de documentos falsos más convincentes o incluso el desarrollo de sistemas sintéticos de voz y rostro para engañar a los sistemas de verificación biométrica. En términos de evolución de la delincuencia, los robos de identidad están avanzando hacia métodos más sofisticados y tecnológicos. Por ejemplo, el phishing y el robo de identidad se han vuelto más sofisticados y, si bien la IA no es la única responsable, ha ayudado a mejorar la personalización de los ataques. Autoridades y empresas están investigando contramedidas para detectar y prevenir estos delitos. Esto incluye el uso de algoritmos para detectar comportamientos inusuales, sistemas de autenticación más sólidos e implementar políticas de seguridad más estrictas. Es importante señalar que los avances tecnológicos pueden haber creado nuevos métodos para cometer fraude, pero también han mejorado la detección y la prevención. Las normas y prácticas de seguridad se adaptan continuamente para hacer frente a los problemas emergentes. Los resultados esperados pueden incluir: Análisis integral de la actual ley de robo de identidad de Ecuador y cómo aborda específicamente temas relacionados con la inteligencia artificial. Investigación en profundidad sobre las tendencias actuales y previsiones de futuro en casos de suplantación de identidad, especialmente aquellos que implican el uso de tecnología de inteligencia artificial. Evaluar las tecnologías de inteligencia artificial utilizadas en casos de fraude, identificando posibles vulnerabilidades de seguridad y áreas de mejora. Explora los impactos sociales del robo de identidad, considerando factores como la confianza pública, la seguridad digital y la conciencia de la privacidad en la era de la inteligencia artificial. Indagar a fondo investigaciones pasadas, leyes actuales y casos relevantes relacionados con el robo de identidad y la inteligencia artificial. Obtenga datos detallados y actualizados sobre casos de suplantación de

identidad en Ecuador, así como información sobre el uso de inteligencia artificial en estos contextos. Realizar un análisis legal detallado de las leyes de robo de identidad e inteligencia artificial en Ecuador. Además, analizamos las tecnologías de inteligencia artificial utilizadas en estos casos.

**¿El delito de suplantación de identidad, se puede cometer con el uso de inteligencia artificial en el Ecuador?**

### 1.3. Objetivo General

Determinar que la conducta del uso fraudulento de la inteligencia artificial genera el delito de suplantación de identidad en Ecuador.

### 1.4. Objetivos Específicos

- Demostrar, que con el uso de la inteligencia artificial se accede sin autorización del titular a la base de datos de la información de carácter personal.
- Determinar que con el delito de suplantación de identidad realizado con el uso de la inteligencia artificial provoca la vulneración de datos personales
- Establecer grados de responsabilidad legal sobre el uso de los datos personales a los tenedores de la información.

### 1.5. Justificación

El análisis del delito de suplantación de identidad es fundamental debido a su creciente relevancia en el contexto actual, especialmente con la expansión del uso de la tecnología y la posible incorporación de la Inteligencia Artificial (IA). En Ecuador, como energías de seguridad: La inversión en tecnologías de seguridad robustas, incl muchos otros lugares, la suplantación de identidad ha evolucionado con el avance tecnológico, presentando desafíos adicionales que requieren una comprensión profunda y estrategias específicas para su prevención y control:

1. Relevancia del análisis del delito de suplantación de identidad: La suplantación de identidad implica la usurpación de la identidad de una persona para cometer fraudes, acceder a información privada o llevar a cabo actividades ilegales. Esto puede tener repercusiones devastadoras en la vida personal, financiera y social de los individuos afectados. Es crucial entender la naturaleza cambiante de este delito para desarrollar medidas efectivas de prevención y respuesta.

2. Impacto de la Inteligencia Artificial: La IA ha revolucionado la forma en que interactuamos con la tecnología, pero también ha presentado desafíos en términos de seguridad. Los avances en IA podrían ser utilizados para mejorar los métodos de suplantación de identidad, generando perfiles más convincentes y difíciles de detectar. El uso de algoritmos sofisticados podría permitir la manipulación de datos biométricos o la creación de perfiles falsos más convincentes.
3. Posible incremento en la suplantación de identidad: La integración de la IA en herramientas y sistemas digitales podría potencialmente aumentar la sofisticación de los métodos de suplantación de identidad. Esto incluye la capacidad de generar rostros falsos realistas, imitar voces humanas, y manipular datos biométricos. Si no se implementan medidas de seguridad efectivas y se fortalecen las leyes y regulaciones, existe el riesgo de un aumento significativo en los casos de suplantación de identidad. En Ecuador, como en cualquier país, es esencial desarrollar estrategias integrales que aborden estos desafíos:

- Actualización de leyes y regulaciones: Es crucial adaptar las leyes para abordar las nuevas formas de suplantación de identidad facilitadas por la IA y garantizar sanciones adecuadas para los infractores.
- Educación y concienciación: La sensibilización pública sobre los riesgos de la suplantación de identidad y las medidas de seguridad digital es fundamental para empoderar a las personas y empresas para proteger sus datos.
- Desarrollo de tecnología sistemas de verificación biométrica avanzada y detección de actividad sospechosa, es esencial para mitigar el riesgo de suplantación de identidad. En resumen, el análisis y la comprensión del delito de suplantación de identidad, especialmente en el contexto de avances en la IA, son cruciales para desarrollar estrategias efectivas de prevención y protección en Ecuador y a nivel global.

# 2. Marco teórico

## 2.1. Los Sistemas Informáticos

Primeramente, la definición del sistema informático, según el Convenio de Budapest en el capítulo 1, Art. 1: “Se entiende como todo dispositivo aislado o

conjunto de dispositivos interconectado o relacionados entre sí, cuya función o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa". (Consejo de Europa, 2001)

Según la Facultad de Ciencias y Tecnología de la Universidad Isabel I dentro de su portal web describe al Sistema Informático como el conjunto de los elementos físicos y lógicos encargados de recibir, guardar y procesar datos para convertirlos en resultados. El sistema informático se compone de Hardware y Software; refiriéndose a la primera como la parte tangible y la última a la parte lógica. (Sistemas informáticos (SI): qué son, características y tipos, 2023)

Por otro lado, hay que tener en cuenta que estos sistemas informáticos pueden ser vulnerables, de acuerdo a lo que establece Obando & Vásquez (2022):

> Los sistemas informáticos sin importar sus características tecnológicas hardware, como por ejemplo el procesador con su capacidad de procesamiento de la información, al conectarse a una red de comunicaciones, como es el internet, es vulnerable a cualquier ataque informático ya que la forma como acceden y transmiten información en este tipo de redes no depende de esas características tecnológicas sino del medio de transmisión, y principalmente de la estructura en la cual los datos viajan de un dispositivo a otro (p.72).

En resumen, el sistema informático se considera como el conjunto de componentes hardware y software diseñados para realizar tareas específicas mediante el procesamiento de datos. Los sistemas pueden ser distintos dependiendo de los dispositivos tales son: teléfonos móviles hasta complejas redes de servidores en centros de datos. La función principal es procesar la información de entrada y consecutivamente obtener resultados útiles para los usuarios, sin embargo, puede verse frágil ante ataques informáticos debido a la transmisión de información a través de la red. Los datos que se envían y reciben pueden ser interceptados por terceros no autorizados, lo que podría exponer la seguridad y la integridad del sistema.

## 2.2. La Red Internet

La internet surge en el año de 1969 con el nombre de ARPANET, se concibe del interés militar, cuyo objetivo era eliminar la dependencia de un Ordenador Central y erradicar las vulnerabilidades de las comunicaciones militares norteamericanas durante la guerra fría. Se establece la primera conexión de computadoras entre tres universidades de California y otra en Utah (EE. UU). Consistía en un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP (Transmission Control Protocol/Internet Protoco), que son las normas para introducir los datos a la red y así garantizar una red lógica única al alcance mundial. (Sevilla Robles, 2023).

Dicho de otra manera, son diferentes ordenadores interconectados globalmente para facilitar el acceso a datos y programas desde cualquier parte del mundo convirtiéndose en una herramienta para intercambiar y esparcir información y a su vez de interacción entre las personas con ayuda de sus ordenadores de diferentes puntos geográficos, utilizando un lenguaje común.

Hoy por hoy, la internet es un medio para la realización de distintas actividades ya que, nos ofrece sitios web, blogs, redes sociales, comercio, banca móvil, correos electrónicos, almacenamientos y muchas otras cosas que se utilizan en la cotidianidad.

## 2.3. La Inteligencia Artificial

Según Hermosilla, (2023) define a la Inteligencia Artificial (IA) como los "sistemas de software y potencialmente también de hardware creados por el ser humano, que, ante un objetivo complejo, operan en un entorno físico o digital. Estos sistemas perciben el entorno mediante la colección de datos, los interpretan y procesan la información obtenida para decidir las mejores acciones a seguir con el fin de alcanzar el objetivo establecido".

La inteligencia artificial (IA) se refiere a la capacidad de las máquinas o sistemas para realizar tareas que normalmente las realizaría el ser humano como el aprendizaje, la percepción, el razonamiento y la resolución de problemas. La IA se aplica en una amplia gama de campos, como la robótica, el procesamiento del lenguaje natural, la visión por computadora, los sistemas de recomendación, entre otros. El objetivo es crear sistemas que puedan aprender de los datos, adaptarse a nuevas situaciones y realizar tareas de manera autónoma.

La IA utiliza diferentes técnicas para lograr cumplir su función, una de las más conocidas es la técnica del Big Data (BD) que consiste en una gran base de datos, que, acumulada con el pasar del tiempo necesitan de un tratamiento de análisis no convencional por su extenso almacenamiento de datos por el cual, se requiere de muchos terabytes para dicho almacenamiento de información que se puede convertir en conocimiento si se le da el tratamiento adecuado.

De modo que, se considera que la Big Data es la principal esencia de la IA por permitir la extracción y manejo de datos que va a permitir pronosticar conductas a futuro de las personas y a la obtención de información a partir de la proporcionada. En la actualidad la BD y la IA trabajan de la mano para la producción y recolección de información de distintas fuentes, haciendo un análisis de metadatos (información que describe otros datos), datos personales (sensibles o no), otros datos no personales que tiene origen durante el desempeño de actividades laborales u otras actividades externas.

## 2.4. El Impacto Del Uso De Internet Y Redes Sociales A Partir De La Pandemia De 2020

Con el avance de la tecnología en los últimos tiempos el uso de la red y de sistemas informáticos son más frecuentes en todos los ámbitos, como el laboral, el educativo y el social. En 2020, con el inicio de la pandemia se dio paso al confinamiento prolongado de la población en sus hogares para evitar el contacto físico y frenar los contagios de Covid-19, en consecuencia, muchos establecimientos comerciales, educativos y laborales tuvieron que detener sus actividades diarias, paralizando prácticamente al mundo entero.

Ante la situación se dio la necesidad de utilizar diferentes dispositivos electrónicos que permitía continuar con las actividades diarias de manera remota a los lugares de trabajo. Este fenómeno se conoció como teletrabajo, que consistía en conectarse a través de internet utilizando programas para realizar tareas de forma virtual. Aunque este método no era equivalente al trabajo presencial en una oficina o un establecimiento adecuado, permitió que muchas actividades continuarán desarrollándose. Además, el uso de redes sociales como Facebook, Instagram, WhatsApp y YouTube aumentó considerablemente, ya que muchos usuarios aprendieron a utilizarlas como un medio de comercialización, teniendo como resultado a pequeños emprendedores y grandes empresas que vieron en la comercialización

electrónica una oportunidad para promocionar sus productos o servicios y obtener nuevos clientes.

Según un informe de We Are Social & Hootsuite (Kemp, 2022), existen 4620 millones de usuarios en redes sociales, equivalentes al 58% de la población mundial, con un aumento del 1% diario en la contratación de internet. Estos usuarios dedican alrededor de 7 horas diarias a las redes sociales o a realizar otras actividades en la web. También queda demostrado la efectividad de este tipo de publicidad por medio de las redes sociales pues, 1 de cada 4 usuarios entre las edades de 16 a 64 años descubren nuevas marcas, productos o servicios a través de los anuncios; y 7 de cada 10 usuarios pagan por algunos de estos productos y servicios visualizados por medio de la red.

A medida que la tecnología ha tenido un avance muy significativo y beneficioso, también trae consigo un lado negativo, en cuestión encontramos que los grupos delictivos también aprovechan las oportunidades que nos ofrece la internet, el claro ejemplo: la utilización de las redes sociales para cometer ciberdelitos o delitos informáticos.

## 2.5. Delitos Informáticos

Los delitos informáticos o también conocidos como ciberdelitos son los actos ilícitos que se llevan a cabo por medio de las Tecnologías de la Información (TI). Así mismo, es la acción antijurídica culposa o no culposa, es decir, la existencia de la intención o sin ella, que cause daño directo a las personas, entidades o al bien jurídico protegido. En esa misma línea, Acosta, Benavides, & García (2020), expresa en su trabajo de investigación: “Los delitos informáticos, son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets” (p.351)

(Mayer Lux & Calderón, 2020) expresan que el ciberdelito tiene origen en estafas informáticas que se relacionan con transferencias electrónicas de fondos, el fraude informático es centro de los cibercriminales por el impacto económico potenciado por el auge del comercio electrónico.

En el 2021, Saltos Salgado, Robalino Villafuerte, & Pazmiño Salazar han concluido que hay ciertas características para definir un delito informático como los factores criminógenos de cuello blanco, aprovechando oportunidades dentro de

funciones y organizaciones del sistema tecnológico y económico, lo que puede causar pérdidas económicas significativas. Estos delitos pueden llevarse a cabo en fracciones de segundo sin necesidad de presencia física, son más sofisticados y ocurren con frecuencia en el ámbito militar, y presentan grandes desafíos para su comprobación debido a su carácter técnico. No siempre existe la intención de causar daño, pero su proliferación creciente requiere una regulación urgente. (p. 346).

La internet tiene información al alcance de cualquier persona, que, con el uso inadecuado se puede llegar al cometimiento de delitos informáticos tales como la suplantación de identidad, falsificación de documentos, acoso no consentido a un sistema informático, interceptación ilegal de datos, revelación ilegal de datos entre otros; utilizando técnicas como ransomware, el phishing, los ataques de denegación de servicio entre otras. Los delitos informáticos cada vez son más sobresalientes y frecuentes a partir de la pandemia, afectando a individuos y grandes corporaciones por lo cual se debe de invertir en ciberseguridad para la protección de los sistemas y datos importantes.

La legislación sobre ciberdelitos está en constante evolución, con leyes más estrictas y cooperación internacional para combatir estas amenazas. A pesar de estos esfuerzos, el desafío sigue siendo significativo debido a la naturaleza global y anónima de Internet, lo que dificulta la identificación y enjuiciamiento de los perpetradores. Además, se están promoviendo la educación y la concienciación sobre ciberseguridad como medidas preventivas esenciales para reducir el riesgo de ser víctima de delitos informáticos.

### *2.5.1. Delitos Informáticos Reconocidos Dentro De Nuestra Legislación Ecuatoriana Y El Tratado Internacional De Delitos Informáticos*

Según Saltos Salgado, et al. (2021) establece que los delitos informáticos han experimentado un crecimiento significativo en los últimos años en América Latina, subrayando la relevancia y necesidad de su estudio. Además, en Ecuador se empezó a hablar de delitos informáticos en 2009, registrando un total de 3,143 casos hasta 2013, a pesar de que se estima que el 80% de estos delitos no son reportados. En términos de índice delictivo, Ecuador se sitúa en el tercer lugar, después de México con un 92% y Bolivia con un 85%. Según la ONU, esto es consecuencia de la falta de una cultura de denuncia.

El Convenio sobre la Ciberdelincuencia (Budapest) o Tratado de Delitos Informáticos es el tratado internacional que se enfoca en los delitos que se llevan a cabo a través de medios o sistemas informáticos y de la internet. Este Convenio establece la regulación y política penal para la ciberdelincuencia, es decir, que adecua una legislación para el tratamiento de los delitos informáticos que perjudican a la sociedad y el patrimonio; y de la misma manera pretende la modernización de la cooperación entre países.

Dentro de este tratado Internacional se encuentran algunas conductas ilícitas llevadas a la práctica tras el uso del internet y de las tecnologías de la comunicación. Macías-Lara, et al., (2022) clasifica los delitos informáticos a nivel general por grupos que van de la siguiente forma: 1. Fraude informático; 2. Acoso o espionaje informático; 3. Sabotaje informático; 4. Pornografía infantil; 5. Infracción a la propiedad intelectual y derechos de autor; y 6. Interceptación no autorizada. Cada grupo engloba otros delitos informáticos que son representativos y que conviene destacar, así como:

- **Acceso ilícito**: Consta como un tipo de fraude bastante común que consiste en engañar a una persona y en consecuencia dañar su patrimonio. Los delincuentes utilizan medios electrónicos, redes sociales o llamadas telefónicas para obtener información confidencial y estafar a su víctima.
- **Interferencia de datos**: Esta conducta afecta la integridad y disponibilidad de la información, modificándose, dañándose, eliminando o alterando datos informáticos sin autorización y se considera una actividad delictiva en el marco de la ciberdelincuencia.
- **Interferencia en el sistema**: Es la acción de bloquear, interrumpir o dañar el funcionamiento de un sistema informático sin permiso. Este tipo de delito funciona a través de la introducción de malware, la saturación de servicios a través de ataques de denegación de servicio, o cualquier otra forma de manipulación que obstaculice el correcto uso del sistema.
- **Violaciones de seguridad de red:** La violación a la red es el acceso ilícito a una red informática de forma maliciosa para obtener información confidencial o comprometer la seguridad.
- **Uso indebido de dispositivos:** Se refiere al uso de los dispositivos; inclusive su fabricación, distribución, venta, importación, obtención o posesión para acceder a sistemas informáticos sin autorización.

- **Ciberacoso:** Se hace uso de los medios digitales para acosar a una persona o más de forma anónima en un lapso de tiempo. Implica revelar información que puede ser cierta o falsa, además de amenazas hacia al individuo.
- **Falsificación informática**: Es la conducta reconocida por manipular datos electrónicos para hacer que parezcan auténticos, con el propósito de engañar a las personas para adquirir beneficios ilegítimos.
- **Delitos relacionados con el contenido**: Delito relacionado con contenidos sexuales, así como la Pornografía infantil, del mismo modo incluye su producción, oferta, distribución o posesión del contenido.

Estos delitos informáticos tienen una similitud clave, esto es la conducta ilícita, engañosa, y fraudulenta para la obtención de una ganancia mediante el uso de la tecnología y la red, afectando a bienes jurídicos protegidos como el patrimonio; los derechos como la privacidad, la seguridad y la integridad de los datos y sistemas informáticos.

En nuestro Ordenamiento Jurídico Ecuatoriano para que se configure un delito Informático debe cumplir ciertos requerimientos. “La tipificación del delito informático en la Ley Penal responde a elementos tales como el sujeto, medio y objeto” (Saltos Salgado, et al., 2021, p. 344), siendo el sujeto el autor que cometa la conducta ilícita (que podría ser cualquier persona); el medio se refiere al sistema informático que se utilice y el objeto es el beneficio económico que de cualquier forma es ilícito.

La influencia de los delitos informáticos requiere de una regulación efectiva para enfrentar la vulneración de los derechos de la víctima. Las leyes y normativas vigentes deben reformarse constantemente a las necesidades de la población, debido a las nuevas amenazas que se presentan en el medio digital frente a los derechos de los ciudadanos. Hay que enfatizar que para obtener mejores resultados al combatir la ciberdelincuencia es importante la cooperación internacional puesto que, estos delitos superan las fronteras nacionales.

### *2.5.2. Técnicas Y Formas Utilizadas Para El Cometimiento De Los Delitos Informáticos*

Cualquier individuo puede convertirse en un ciberdelincuente puesto que no existen los esfuerzos físicos, solo se necesita tener cualidades intelectuales para la

manipulación de los sistemas informáticos y la tecnología. El ciberdelincuente tiene a disposición una gran cantidad de dispositivos del cual se vale para consumar el delito, igualmente cada vez son más las técnicas o formas para traspasar las medidas de seguridad de los sistemas. De acuerdo a Aparicio-Izurieta (2022) los que practican este tipo de delitos utilizan el comercio electrónico, perfiles falsos, vínculos que contienen virus informáticos, páginas web fraudulentas, etc. ya que de esta forma se dificulta el reconocimiento de la persona que fraudulentamente actúa en beneficio propio o de un tercero.

Los sistemas de seguridad que se utilizan para la protección de datos pueden verse perjudicados por distintos ataques al sistema, uno de los modos para producir estos ataques a la ciberseguridad es la introducción de Malware, proviene de “los términos en inglés *malicius software*, a cualquier tipo de código escrito en lenguaje informático, que al ejecutarse realiza acciones dañinas en un sistema de manera intencional y sin el conocimiento del usuario o propietario de dicho sistema” (Mariano Díaz, 2020, p.3). Al malware también se le puede conocer como virus informáticos, esto quiere decir que utiliza códigos sistematizados para acceder a sistemas para luego pasar a otros, creando una cadena sucesivamente.

En el grupo de los *Malware* se encuentra otros tipos de virus con funcionalidad diferente, tal es el caso de los llamados *gusanos*, son virus informáticos que encubiertos dentro del sistema o programa; lo que hacen es procesar, modificar o eliminar datos, a diferencia de este el malware común se puede regenerar y esparcirse mientras que los gusanos sólo se instalan en un lugar en específico.

También tenemos la *Bomba lógica* o cronológica, se le da este nombre porque el virus actúa luego de cumplirse una condición o determinado tiempo. Debe tenerse conocimientos especializados para llevar a cabo este tipo de programación que puede destruir o modificar datos en el futuro.

Por otro lado, tenemos el *Hacking*, muy frecuentemente se habla de los hackers o piratas informáticos, según la página web del Ministerio de Educación los Hackers son quienes tienen el conocimiento suficiente para ingresar y manipular los sistemas digitales sin ser reconocidos o detectados.

El *troyano* es un virus informático que no se reproduce, pero puede causar daño al sistema al tomar el control una vez infectado. Crea puertas traseras que permiten conexiones no autorizadas y pasar desapercibido. Puede crear, modificar, eliminar y encriptar datos. Se esconde en programas aparentemente inofensivos, de ahí su

nombre, en referencia al caballo de Troya que busca pasar inadvertido.

El *Spyware, este virus* captura información privada como datos personales, contraseñas, direcciones de correos electrónicos, etc. del equipo afectado y la envía sin el consentimiento del usuario.

También está el *bot malicioso* es un tipo de malware cuyo objetivo es robar información o infectar un dispositivo que se utiliza con frecuencia. A menudo, se propaga a través de sistemas mediante código malicioso.

El *Ransomware*, proviene de los términos ransom (rescate) y software. El virus lo que hace es encriptar un sistema informático para luego demandar una recompensa por el funcionamiento de dicho sistema, mediante una clave.

Hay muchos otros tipos de virus que operan similar o tienen una funcionalidad variada, pero, todos con el mismo fin: El de ingresar fraudulentamente a un sistema informático, evadiendo toda seguridad para posteriormente perjudicar dicho sistema y obtener cierta información personal y de gran valor, así como, modificarla o eliminarla.

Por último, tenemos existen otras técnicas sólidas como el *Relleno de credenciales (Credential stuffing)*, los hackers consiguen las credenciales de los usuarios para luego usarlas con otros sistemas mediante el uso de herramientas automatizadas. Así mismo, tenemos el *Phishing o suplantación de identidad*, hasta en la actualidad se sigue utilizando por su gran efectividad ya que opera por medio de correos electrónicos, donde se persuade a la víctima para que haga clic en enlaces maliciosos y proporcione sus credenciales de acceso legítimas, posterior a esto el atacante los utiliza en otros sitios web para creación de nuevos perfiles o identidad falsa.

### *2.5.3. Medidas De Prevención Para Combatir Los Delitos Informáticos*

Toala Indio (2021) dentro de investigación sobre los delitos informáticos frecuentes en el Ecuador establece que en varios países ven necesaria la prevención de los ciberataques, existiendo un ranking establecido por la Unión Internacional de Telecomunicaciones de 193 países comprometidos a enfrentar esta problemática, Ecuador por su parte se en encuentra en el puesto 66 a nivel mundial como parte de este cometido. Además, expone que en nuestro país sí existen estudios realizados sobre la ciberseguridad, por lo que se debería promulgarse capacitaciones de tipo educativo a nivel nacional para la comprensión de los riesgos que trae los ataques a

la seguridad informática. (p,p. 3-4).

Como medidas para mantener el orden social y prevenir de ser víctimas de delitos informáticos, se cree indispensable la concientización a toda la ciudadanía respecto al tema, de manera que la población evite caer en estafas y engaños; así pues, se recomienda ciertas medidas como: **1.** Tener actualizados los sistemas operativos y aplicaciones de los dispositivos, así como el uso de antivirus confiables; **2.** Cuando se tenga correos en Spam es mejor eliminarlos inmediatamente, no ingrese a enlaces sospechosos pueden llevar a adquirir ciertos virus, en cuanto a las redes sociales tener en cuenta los datos personales que comparte para evitar ser blanco fácil para los delincuentes: **3.** Las cuentas bancarias solo se deben abrir en un dispositivo personal, de igual forma las contraseñas deben ser fuertes utilizando mayúsculas, minúsculas, numeración y algún carácter. No repita contraseñas para varias cuentas personales, ni mucho menos compartirlas con terceros; 4. Siempre tenga una copia de seguridad como respaldo en caso de perder información por virus informáticos; 5. No crea en publicidad de internet que ofrecen premios o dinero, suelen ser engañosas, siempre que descargue alguna aplicación asegúrese de que sea de sitios confiables (tiendas oficiales); 6. Utilice su ubicación sólo cuando sea necesaria, de igual forma tener precaución al activar y conectarse a una red WIFI en especial las que se encuentran sin protección (Macías-Lara, et al., 2022, p. 241).

"La necesidad de fomentar la denuncia de estos actos para contribuir a la prevención y persecución de estos actos ilegales" (Diaz Basurto, Ojeda Sotomayor, Cajas Parraga, & Cabrera Ripalda, 2023, p. 752). Las estafas en línea ponen en riesgo el derecho de los datos personales o información sensible, es por eso la importancia de fomentar la prevención ante los ciberdelitos. Estos autores dentro de su investigación hacen referencia acerca de las Complejidades Jurídicas de los delitos informáticos y de la legislación actual frente a la evolución digital, en efecto se considera que deben abordar estrategias más efectivas para el tratamiento de los delitos informáticos y la ciberseguridad.

Diaz Basurto, et al., (2023) exponen que el fiscal Edwin Pérez, especialista en delitos informáticos, indica que en el Ecuador existe dificultad en el momento de la investigación de delitos propiciados por el uso de la tecnología (p. 752). Es cierto que Ecuador se ha adaptado al Convenio de Budapest, lo que ha permitido que su legislación reconozca y regule diversas actividades delictivas realizadas a través de sistemas informáticos e Internet. Sin embargo, aún se necesitan más recursos para

enfrentar eficazmente este tipo de delitos y sus consecuencias. Hay que recalcar que el delito informático cruza fronteras, por ello, la cooperación internacional es crucial para fortalecer las normativas que protegen los derechos de datos personales y privacidad.

Sin embargo, Ecuador no forma parte de convenios internacionales sobre el cruce de datos informáticos, tal es el caso entre Estados Unidos y Europa. En consecuencia, se encuentran complejidades a la hora de localizar las cuentas fraudulentas o las direcciones IP desde donde se comete el ataque o la sustracción de información personal, y el proceso para descubrirlo puede durar meses. Por ende, impulsar la reforma del Código Orgánico Integral Penal puede ser oportuno para resguardar la privacidad, la información personal, la seguridad y el patrimonio debido al desarrollo digital.

El marco legal ecuatoriano requiere fortalecerse y expandirse, incorporando nuevas disposiciones que sancionen más severamente las acciones u omisiones llevadas a cabo mediante tecnologías informáticas, electrónicas y redes de información. Esto tiene como objetivo abarcar la mayor cantidad posible de formas de amenaza contra la integridad del Estado y la sociedad a través de la informática, y así reforzar el principio de seguridad jurídica.

## 2.6. La Protección De Datos Y Privacidad

Según Mok (2020), “El aspecto de privacidad y, más específicamente, lo relacionado con la protección de datos personales es de gran importancia en el ambiente de comercio electrónico. Esto debido a que en cualquier transacción comercial que el consumidor realiza a través de una página Web, el mecanismo mayormente utilizado es por medio de contratos de adhesión, que se basan en formularios prediseñados por el proveedor, y en los cuales, se solicitan información personal al consumidor” (p. 116) .Desde la creación de los sistemas informáticos y la primera red de Internet en el lapso del tiempo su evolución ha sido muy constante, dando como resultado un impacto de gran relevancia en todos los ámbitos de la vida cotidiana. La actualidad de hoy es la era digital, la gran mayoría de trabajos y actividades funcionan por medio de los sistemas informáticos y diversas tecnologías que se tienen a disposición.

La tecnología tiene su lado positivo, pero también trae consigo el lado negativo, y es que la era digital da paso a los delitos informáticos o ciberdelitos, es decir, los

delincuentes han hallado la manera para delinquir por medio de las tecnologías de comunicación y de la red, obteniendo un beneficio económico ilícito y en consecuencia afectando a individuos y personas jurídicas, así como a los bienes protegidos como el patrimonio y a la vulneración del Derecho a la identidad y la privacidad.

Nuestra constitución es de manera muy garantista de derechos y uno de los derechos que protege y garantiza a los ciudadanos es el derecho de la protección de datos, el de identidad y privacidad. Sin embargo, con la repercusión que ha tenido los delitos informáticos la legislación vigente no es lo bastantemente efectiva para la regulación de estos delitos y la protección de las víctimas, debido a que, existen complejidad para la investigación de los delitos ejecutados con el uso de la tecnología puesto que, solo es cuestión de segundos para consumar un ciberdelito por la rapidez que proporciona los medios, además de la dificultad de descubrir a los ciberdelincuentes detrás de cuentas falsas o el rastreo de las direcciones IP por la cual se realiza el ataque a las víctimas.

Existe la necesidad de reformar y fortalecer la normativa penal respecto a los delitos informáticos en especial el de la Suplantación de Identidad por medio de software de inteligencia artificial, para proteger los datos personales, la privacidad y el patrimonio. Incorporándose nuevas sanciones que penalicen las formas de delinquir; acciones u omisiones por medio de dispositivos informáticos y de la red, teniendo como efecto el aumento de la seguridad jurídica.

El uso descomunal de la inteligencia Artificial para suplantar la identidad de otra persona está teniendo una gran incidencia en los últimos años, por lo que se requiere medidas efectivas para contrarrestar esta problemática, así como del análisis amplio del marco legal en relación a la suplantación de identidad y otros delitos informáticos que van de la mano.

Por último, se reconoce que los delitos informáticos traspasan fronteras internacionales, por lo que se requiere de la cooperación entre países para combatir las consecuencias y daños hacia la víctima y su patrimonio.

Por otro lado, la Constitución de la República del Ecuador establece en su artículo 66 numeral 19 lo siguiente:

**Artículo 66.-** se reconoce y garantizará a las personas:

> **19.** El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución, 2008)

La Constitución de 2008 es muy garantista y protege los datos e información personal, lo cual es crucial debido al riesgo de exposición a nuevas tecnologías. Actividades que antes se realizaban presencialmente ahora se llevan a cabo virtualmente gracias a la tecnología y los sistemas informáticos. Por esta razón, la protección de datos y privacidad cobra mayor importancia. Esto implica la gestión segura de la información personal que las organizaciones recopilan y utilizan en bases de datos. Si no se maneja adecuadamente, puede representar un riesgo significativo para los usuarios. Es esencial fortalecer las medidas de seguridad para prevenir posibles abusos y proteger la integridad de los datos personales la normativa vigente encargada de las regulaciones de todo procedimiento y tratamiento referentes a los datos personales, esto es el acceso y su protección.

La ley orgánica de protección de datos personales es otra normativa vigente encargada de las regulaciones de todo procedimiento y tratamiento referentes a los datos personales, esto es el acceso y su protección. En el Capítulo 1, artículo 1 expresa lo siguiente:

> **Artículo 1.- Objeto y finalidad. -**El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (Asamblea, 2021).

Para tener claro el concepto de los datos personales hay que sostener que es toda la información sirve para la identificación de una persona, por ejemplo, sus nombres

completos, número de identificación, números de teléfonos, direcciones de correos electrónicos, y otros datos relacionados a la persona. Cabe recalcar que estos datos al ser intrínsecos de las personas también son privados. La privacidad a su vez es un derecho que tienen todos los individuos, dicho de otra manera, la persona tiene el derecho de controlar toda su información personal, como los utiliza y comparte con otros individuos o personas jurídicas.

La protección de datos es consecuencia de las irregularidades que surgen a partir de compartir información personal en la red o sistemas informáticos y consecuentemente afecta a la persona. La protección de datos son todas las medidas y controles que se pueden tomar para respaldar y salvaguardar los datos personales contra el acceso, divulgación, alteración y destrucción no autorizadas.

## 2.7. La Suplantación De Identidad Dentro Del Código Orgánico Integral Penal De Ecuador

"Los delitos informáticos a nivel internacional y nacional han aumentado de manera significativa durante y después de la pandemia, tal es el caso que los reportes de los diarios, redes sociales y noticias televisivas del Ecuador menciona que los casos más comunes de este tipo es la suplantación de identidad." (Macías-Lara, et al., 2022, p.231)

La suplantación de identidad por mucho tiempo ha sido uno de los delitos consecuentes en Ecuador, así como en otros países. Este delito conlleva a una persona utilizar la identidad de otra, regularmente para obtener algún beneficio monetario; y por defecto cometer fraudes. La suplantación de identidad ha tomado diversas formas teniendo en cuenta los cambios dependientes de la tecnología; convirtiéndose en un ciberdelito (phishing) en el que los delincuentes aprovechándose de los correos electrónicos, mensajes de texto, llamadas telefónicas y redes sociales, logran engañar a las personas y obtener información personal como números de identificación, cuentas personales y contraseñas; y de esa forma abrir cuentas bancarias, solicitar préstamos y realizar compras afectando a individuos, así como a empresas.

Las consecuencias para la persona o la entidad son irrefutables, en primer caso está la pérdida económica que enfrentan las víctimas que se consideran muy significativas debido a las compras no autorizadas, las transferencias de dinero y préstamos ficticios. También tenemos el daño que repercute en la reputación de la

víctima ya que, se ha utilizado su identidad para perpetrar otros delitos y consecutivamente la llegada de problemas legales que se puede verse involucrada por las actividades ilícitas. Este delito está tipificado en el Código Orgánico Integral Penal, en el Articulo 212 relata lo siguiente: “La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, *será sancionada con pena privativa de libertad de uno a tres años*” (COIP, 2021).

La legislación en Ecuador sobre suplantación de identidad es limitada, sin embargo, trata de regular de acuerdo a las necesidades que tiene la población. Pero es motivo suficiente para fomentar reformas para fortalecer las leyes que penalizan este delito y protege a las víctimas, pues, se está en constante desarrollo en todos los ámbitos. Las autoridades competentes toman medidas para controlar la suplantación de identidad, como concienciar a las personas sobre sus riesgos y consecuencias. Es de relevancia proteger la información personal, siendo precavidos con los datos compartidos en línea, creando contraseñas fuertes y el uso de sistemas de seguridad cualificados, autenticación de dos factores y cifrado de datos.

### 2.7.1. El Delito De Suplantación De Identidad En Ecuador Durante Los Últimos Años

La fiscalía general del Estado lleva un registro íntegro de los delitos que se reportan a diario en Ecuador gracias al Sistema Integrado de Actuaciones Fiscales (SIAF), donde se recolectan todos los datos y estadísticas de los delitos consumados o simplemente en tentativa.

La fiscalía nos aporta las estadísticas respecto al delito de Suplantación de Identidad desde el año 2019 hasta la presente para evaluar la frecuencia con la cual se comete este delito tanto a nivel nacional como en la provincia del Guayas.

**Tabla 1.**

*Noticias del delito de suplantación de identidad a nivel nacional registradas en el Sistema SIAF.*

| PROVINCIA | CONSUMADO | | | | | | TENTATIVA | | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | |
| AZUAY | 176 | 154 | 263 | 146 | 137 | 44 | 1 | 1 | | 1 | | 1 | 924 |
| BOLIVAR | 18 | 24 | 19 | 22 | 40 | 13 | | | | | | | 136 |
| CANAR | 29 | 15 | 29 | 35 | 30 | 16 | | | | | | | 154 |
| CARCHI | 35 | 26 | 26 | 26 | 20 | 9 | | | 1 | 1 | | | 144 |
| CHIMBORAZO | 46 | 47 | 60 | 51 | 54 | 35 | 1 | | | | 1 | | 295 |
| COTOPAXI | 62 | 48 | 54 | 52 | 82 | 24 | | | 1 | | 1 | | 324 |
| EL ORO | 182 | 162 | 236 | 232 | 184 | 113 | | 3 | 2 | | | 4 | 1.118 |
| ESMERALDAS | 53 | 47 | 66 | 91 | 84 | 41 | 1 | | | | | | 383 |
| GALAPAGOS | 11 | 7 | 10 | 4 | 19 | 6 | 1 | | | | | 1 | 59 |
| GUAYAS | 2.129 | 1.448 | 2.076 | 2.116 | 2.363 | 943 | 13 | 10 | 7 | 10 | 11 | 4 | 11.130 |
| IMBABURA | 114 | 79 | 143 | 162 | 168 | 83 | 1 | 2 | | | | | 752 |
| LOJA | 67 | 81 | 133 | 141 | 100 | 53 | | 1 | 1 | | 1 | | 578 |
| LOS RIOS | 100 | 54 | 108 | 130 | 129 | 67 | 2 | | 1 | | | 2 | 593 |
| MANABI | 240 | 171 | 284 | 284 | 281 | 146 | 2 | 1 | | 1 | 1 | | 1.411 |
| MORONA SANTIAGO | 18 | 10 | 15 | 18 | 25 | 4 | | | 1 | | | 1 | 92 |
| NAPO | 16 | 7 | 28 | 25 | 24 | 9 | | | | 1 | | | 110 |
| ORELLANA | 22 | 22 | 25 | 37 | 44 | 17 | | 1 | | | | | 168 |
| PASTAZA | 16 | 8 | 18 | 13 | 16 | 6 | | | | 1 | | | 78 |
| PICHINCHA | 950 | 1.222 | 2.125 | 1.970 | 2.259 | 810 | 8 | 8 | 22 | 6 | 8 | 7 | 9.395 |
| SANTA ELENA | 28 | 35 | 60 | 66 | 71 | 42 | | 1 | | | 2 | | 305 |
| SANTO DOMINGO DE LOS TSACHIL | 52 | 55 | 73 | 106 | 130 | 55 | 1 | | 1 | | | | 473 |
| SUCUMBIOS | 20 | 27 | 42 | 47 | 52 | 11 | | | | | 1 | | 200 |
| TUNGURAHUA | 157 | 119 | 129 | 92 | 116 | 32 | | | | 1 | | | 646 |
| ZAMORA CHINCHIPE | 10 | 13 | 12 | 8 | 17 | 11 | | | | | | | 71 |
| **Total general** | **4.551** | **3.881** | **6.034** | **5.874** | **6.445** | **2.590** | **31** | **28** | **37** | **22** | **26** | **20** | **29.539** |

*Nota. Esta tabla muestra con qué frecuencia se comete el delito de la suplantación de identidad, así como los que no se consumaron a una escala nacional desde el año 2019 hasta la presente fecha.*

**Tabla 2**

*Noticias del delito de suplantación de identidad a de la Provincia del Guayas registradas en el Sistema SIAF*

| Cantón | CONSUMADO | | | | | | TENTATIVA | | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | |
| ALFREDO BAQUERIZO MORENO ( JUJAN ) | | | | 1 | | 2 | | | | | | | 3 |
| BALAO | | 1 | 1 | | | 5 | | | | | | | 7 |
| BALZAR | 8 | 5 | 3 | 6 | 12 | 1 | | | | | | | 35 |
| COLIMES | 1 | | | | | 1 | | | | | | | 2 |
| DAULE | 35 | 46 | 53 | 58 | 74 | 25 | | | | | | | 291 |
| DURAN | 107 | 63 | 89 | 108 | 80 | 39 | | | | 1 | 1 | 2 | 490 |
| EL EMPALME | 48 | 17 | 18 | 15 | 20 | 8 | | | | | | | 126 |
| EL TRIUNFO | 10 | 9 | 5 | 12 | 12 | 4 | | | | | | | 52 |
| GENERAL ANTONIO ELIZALDE (BUCAY) | 2 | | 1 | | 4 | 1 | | | | | | | 8 |
| GUAYAQUIL | 1.825 | 1.212 | 1.776 | 1.775 | 1.992 | 750 | 13 | 9 | 7 | 7 | 10 | 2 | 9.378 |
| LOMAS DE SARGENTILLO | 1 | | | | 2 | | | | | | | | 3 |
| MILAGRO | 33 | 42 | 32 | 42 | 35 | 24 | | | | 1 | | | 209 |
| NARANJAL | 6 | 8 | 14 | 17 | 17 | 16 | | | | | | | 78 |
| NARANJITO | 3 | 1 | 12 | 3 | 6 | 7 | | | | | | | 32 |
| NOBOL | 3 | 1 | 2 | 4 | 2 | 1 | | | | | | | 13 |
| PALESTINA | 1 | | | 1 | 28 | 5 | | | | | | | 35 |
| PEDRO CARBO | 6 | 3 | 8 | 10 | 3 | 2 | | | | | | | 32 |
| PLAYAS | 13 | 14 | 12 | 15 | 25 | 33 | | | | | | | 112 |
| SALITRE | 3 | 1 | 3 | 4 | 3 | 3 | | | | | | | 17 |
| SAMBORONDON | 15 | 17 | 23 | 31 | 26 | 8 | | 1 | | 1 | | | 122 |
| SAN JACINTO DE YAGUACHI | 6 | 7 | 18 | 7 | 11 | 5 | | | | | | | 54 |
| SANTA LUCIA | 2 | 1 | 5 | 3 | 7 | 2 | | | | | | | 20 |
| SIMON BOLIVAR | 1 | | 1 | 4 | 4 | 1 | | | | | | | 11 |
| **Total general** | **2.129** | **1.448** | **2.076** | **2.116** | **2.363** | **943** | **13** | **10** | **7** | **10** | **11** | **4** | **11.130** |

*Nota.* La Tabla 2 recoge las cifras de las veces que se comete el delito de la suplantación

de identidad en cada Cantón, así como la tentativa desde 2019 hasta mayo de 2024.

## 2.8. El Uso Específico De La Inteligencia Artificial Para La Suplantación De Identidad

Como se mencionó anteriormente, la tecnología está en constante evolución, lo que ha llevado a la creación de dispositivos de alta gama y sistemas altamente complejos, incluida la Inteligencia Artificial (IA). La IA es una innovación que puede realizar múltiples tareas que normalmente realizaría un ser humano, como el reconocimiento de voz, el procesamiento del lenguaje, la resolución de problemas y la toma de decisiones, así como el aprendizaje automático.

Loján Alvarado & Cárdenas Villavicencio (2024) en su investigación estudian el lado negativo que se puede reflejar en el mal uso de la IA, por lo que proponen nuevos lineamientos legales y éticos para el uso correcto de estas tecnologías. Binns (2018, como se citó en Loján Alvarado & Cárdenas Villavicencio, 2024) asegura que “Los algoritmos de aprendizaje automático pueden replicar y amplificar sesgos humanos si se entrenan con datos no representativos o discriminatorios” (p. 1968) lo que nos lleva a pensar que de cierta forma esto implicaría la vulneración del derecho de privacidad y seguridad, así como derechos humanos.

La Constitución vigente en el Artículo 66 numeral 28 garantiza a las personas tener una identidad, no solo el nombre y el apellido, sino, también a que esta identidad se vea representada por los rasgos físicos, su origen, creencias, lenguaje y otros aspectos que hacen única a la persona. Ahora bien, con la tecnología en especial la IA es posible la suplantación de identidad por medios digitales, creando una representación completamente igual en todos los aspectos de una persona, inclusive se podría utilizar para cometer actos ilícitos; entonces si es de gran importancia ampliar el marco legal sobre este delito en la era digital para su control y penalización.

Endara-Chamorro, Espinoza-Jiménez, López-Fuel, & Santander Moreno (2024) interpretan al delito de suplantación de identidad como un delito de resultado material o ideal a causa de una conducta ilícita. Por otro lado, manifiestan el uso de la inteligencia artificial en la creación de programas como *Deepfake*, que manipulan voces, imágenes y vídeos, generando incertidumbre en cuanto a las normas jurídicas debido a la lenta adaptación del marco legal al avance tecnológico. Es crucial no solo

buscar soluciones tecnológicas, sino también adoptar enfoques integrales, multifacéticos y legales para regular el comportamiento moral.

### *2.8.1. Deepfake*

Para autores como Barrientos Báez, Piñeiro Otero, & Porto Renó (2024) el deepfake es usado en el medio audiovisual para crear escenas humorísticas utilizando la imagen de personajes reconocidos. Por otra parte, manifiestan que existen el deepfake pornográfico, donde utilizan herramienta de inteligencia artificial para generar imágenes falsas de desnudos o pornografía.

> Los deepfakes deben entenderse como parte del o gendertrolling, término que hace referencia a un troleo específico, dirigido a las mujeres. Más allá de la burla o la risa agresiva contra una víctima más o menos fortuita en la Red, más o menos extendido en el tiempo en función de la reacción de la víctima, el troleo de género suele tener en común su carácter misógino (Mantilla,2013, como se citó en Barrientos Báez, et al., 2024).

Para explica mejor la terminología, según el portal web Lisa Institute los Deepfakes son archivos de vídeo, imagen o voz alterados mediante la IA para hacerlos pasar como originales y de esa forma engañar fácilmente e inducir a las personas al error, la confusión y la desinformación convirtiéndose en un problema grave (Institute, 2024). Existen dos tipos de deepfakes: *1. Deepfaces*, por medio del aprendizaje automático de IA se generan nuevas imágenes o videos a partir de los originales lo cual los hace parecer contundentes; *2. Deepvoices*, se trata de sustituir la voz de una persona en un audio, haciendo que parezca que la persona dijo algo que en realidad no dijo, mediante la falsificación de su voz auténtica. De acuerdo con Endara-Chamorro, et al. (2024) “Para lograr la reconstrucción o cambio del rostro, se necesita de tres etapas, las cuales son: 1. Extracción de la imagen(rostro) 2. Procesamiento del rostro falso 3. Inserción de una máscara dentro del fotograma” (p.246).

### *2.8.2. Casos.*

**2.8.2.1. Redes De Traficantes Emplean Inteligencia Artificial Para Engañar A Familias De Inmigrantes.** En Ecuador, Ecuavisa por medio de su canal de Televisión y en su portal web publica la noticia: ‘‘Con programas de manipulación de imágenes, en Inteligencia artificial, lograron que una migrante, reportada como desaparecida, apareciera hablando en un video y pidieron dinero a sus familiares’’ (Ecuavisa , 2023). Dentro de este reportaje se exponen las nuevas formas para cometer estafas, engañar y robar dinero a los familiares de migrantes. Los coyoteros ‘coyoteros’ conocidos comúnmente en Ecuador y en México como ‘polleros’ se les llaman a los traficantes que organizan viajes supuestamente ‘fáciles’ para el cruce de fronteras entre países, falsificando documentos de identidad o pasaportes; cobrando un excesivo precio.

La delincuencia ha traspasado fronteras, se validan de la tecnología para lograr su cometido; es el caso de los familiares de la migrante Ecuatoriana reportada como desaparecida luego de que intentara cruzar la frontera entre Ciudad Juárez y El Paso, Texas según la boleta que trasmitió la Organización 1800 Migrantes, con la ayuda de la inteligencia artificial los coyoteros pudieron recrear videos de esta persona a partir de unas fotografías y de esa forma solicitar pagos excesivos para el rescate de su familiar. Manipularon fotografías sobreponiendo la foto en una persona como modelo para hacer hablar la foto y de esa manera crear un video muy complejo y real donde la migrante pide su rescate, cuando realmente la mujer desaparecida ya había fallecido en el trayecto de su viaje.

**2.8.2.2. Imágenes Falsas De Reportaros De Ecuavisa Utilizadas Para Estafar A La Ciudadanía.** ‘‘El deepfake es un video, imagen o audio manipulado con inteligencia artificial que imita la apariencia y voz de una persona aparentando que está haciendo o diciendo cosas que en la realidad no ocurrieron’’ (Ecuavisa, 2024). Asi es como se expresa Ecuavisa luego de que se utilizara el logo que les representa y la imagen de algunos reporteros de Televistazo para crear videos e imágenes de supuestos influencers anunciando ciertos negocios de dinero fácil y proyectos de inversión, sirviendose de la imagen del Banco central sin autorización para darle credibilidad legal.

En su portal web explica que el Deepfake esta circulando frecuentemente dentro de las redes sociales para recrear videos o imágenes graciosas, sin embargo, esta tecnia tambien es utilizanda para cometer estafas a la ciudadania, suplantar la identidad de otra persona o crear una nueva para asi obtener un beneficio monetario.

Por otro lado, dan a conocer que las victimas son redirigidas a canales de telegram, a perfiles falsos; y que incluso se clonó el portal web de Ecuavisa para convencer a las personas de facilitar su informacion personal o depositar dinero en alguna cuenta banciera de terceros.

## 3. Metodología del proceso de investigación.

El método cualitativo es el más adecuado para esta investigación porque nos permite analizar de una mejor manera los datos que hemos recolectado a lo largo de la investigación, evaluándose para poder obtener una conclusión adecuada al tema. La metodología a usarse va a ser el método cualitativo. ‘‘Utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación’’ (Sampieri p. 40)

### 3.1. Alcance De La Investigación

**Descriptivo**

Nuestra investigación es explicativa porque vamos a analizar un fenómeno, en el cual se busca analizar las conductas, los grupos y los perfiles de las personas que se pueden ver afectadas por el cometimiento de este delito.

El objetivo del investigador es describir fenómenos, situaciones, contextos y acontecimientos, describiendo cómo se exponen y se declaran. Los estudios descriptivos sirven para precisar las propiedades, características y perfiles de personas, grupos, poblaciones, procedimientos, objetos o cualquier otro acontecimiento que se reduce a análisis.

### 3.2. Delimitación De La Investigación

Se ubica en Ecuador, en la Ciudad de Guayaquil en el periodo 2023.

## 3.3. Población Y Muestra De La Investigación

### *3.3.1. Población*

Según lo que expresa Mejía (2005)

> La población es la totalidad de elementos del estudio, es delimitado por el investigador según la definición que se formule en el estudio. La población y el universo tienen las mismas características por lo que a la población se le puede llamar universo o de forma contraria, al universo, población.

Siguiendo esta definición de Mejía, la población es la totalidad de los elementos de estudios, la suplantación de identidad con el uso de la inteligencia artificial.

### *3.3.2. Muestra*

La muestra es el grupo social al cual se va a entrevistar para poder recolectar los datos para nuestra investigación, en este caso la muestra es, las personas naturales, personas jurídicas, sistemas informáticos, el sistema de justicia, los tenedores de la información. ‘‘El muestreo es un procedimiento por el cual algunos miembros de una población —personas o cosas—, se seleccionan como representativos de la población completa’’ (Guillermina Baena Paz, p.79)

# 4. Métodos empleados.

## 4.1. Entrevista

El método a usar es la entrevista porque el tema requiere de un grupo especializado para ser analizado de mayor profundidad, por la complejidad que tiene este tema. ‘‘Las entrevistas, como herramientas para recolectar datos cualitativos, se emplean cuando el problema de estudio no se puede observar o es muy difícil hacerlo por ética o complejidad (por ejemplo, la investigación de formas de depresión o la violencia en el hogar)’’ (Sampieri, p. 236)

## 4.2. Procesamiento Y Análisis De Resultados

El enfoque a usar es el método cualitativo porque se necesita recolectar información para poder realizar este trabajo, y llegar a una conclusión adecuada, el alcance de

la misma es descriptiva porque se va a describir cómo ocurre este fenómeno y la incidencia que tiene en la sociedad, se desarrolla en la Ecuador en la ciudad de Guayaquil en el año 2023, nuestra población va a ser el delito de suplantación de identidad con el uso de inteligencia artificial y la muestra van a ser todos aquellos factores sociales que se involucran como los tenedores de la información personal, y como método empírico usaremos la entrevista porque es el método que más se relaciona con nuestro tema, al necesitar de personas con experticia en este ámbito.

## 5. Análisis de resultados de la investigación

### 5.1. Discusión De Resultados

Para esta entrevista se realizó en conjunto con expertos en la materia, para poder determinar si es conveniente o no la creación de un nuevo tipo penal, dichas entrevistas nos dejaron posturas muy interesantes respecto a lo que piensan estos expertos sobre la inteligencia artificial como medio para cometer el delito de suplantación de identidad y la responsabilidad de los tenedores de la información personal.

Uno de los encuestados no está de acuerdo con la implementación de grados de responsabilidad a los tenedores de la información personal porque nos indica que ya existe una regulación para ellos que es la LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, la cual efectivamente se encarga de vigilar que las entidades sigan protocolos para regular el uso de estos datos

Los 6 encuestados restantes indicaron que, si están de acuerdo con crear grados de responsabilidad para sancionar a los tenedores de la información, porque indicaron que pese a existir una norma que regula esto, debería ser un tipo penal para que los responsables de los datos personales, tengan mayores parámetros de seguridad y evitar que exista alguna vulneración.

Con los avances tecnológicos que estamos viviendo se debería crear un nuevo tipo penal respecto a la suplantación de identidad que use como medio a la inteligencia artificial, para que de este modo aquellos responsables de la información personales tengan más filtros de seguridad y eviten que sus sistemas informáticos sean vulnerados con facilidad por los ciberdelincuentes.

## 6. Conclusiones

Desde la creación de los sistemas informáticos y la primera red de Internet en el lapso del tiempo su evolución ha sido muy constante, dando como resultado un impacto de gran relevancia en todos los ámbitos de la vida cotidiana. La actualidad de hoy es la era digital, la gran mayoría de trabajos y actividades funcionan por medio de los sistemas informáticos y diversas tecnologías que se tienen a disposición.

La tecnología tiene su lado positivo, pero también trae consigo el lado negativo, y es que la era digital da paso a los delitos informáticos o ciberdelitos, es decir, los delincuentes han hallado la manera para delinquir por medio de las tecnologías de comunicación y de la red, obteniendo un beneficio económico ilícito y en consecuencia afectando a individuos y personas jurídicas, así como a los bienes protegidos como el patrimonio y a la vulneración del Derecho a la identidad y la privacidad.

Nuestra constitución es de manera muy garantista de derechos y uno de los derechos que protege y garantiza a los ciudadanos es el derecho de la protección de datos, el de identidad y privacidad. Sin embargo, con la repercusión que ha tenido los delitos informáticos la legislación vigente no es lo bastantemente efectiva para la regulación de estos delitos y la protección de las víctimas, debido a que, existen complejidad para la investigación de los delitos ejecutados con el uso de la tecnología puesto que, solo es cuestión de segundos para consumar un ciberdelito por la rapidez que proporciona los medios, además de la dificultad de descubrir a los ciberdelincuentes detrás de cuentas falsas o el rastreo de las direcciones IP por la cual se realiza el ataque a las víctimas.

Existe la necesidad de reformar y fortalecer la normativa penal respecto a los delitos informáticos en especial el de la Suplantación de Identidad por medio de software de inteligencia artificial, para proteger los datos personales, la privacidad y el patrimonio. Incorporándose nuevas sanciones que penalicen las formas de delinquir; acciones u omisiones por medio de dispositivos informáticos y de la red, teniendo como efecto el aumento de la seguridad jurídica.

El uso descomunal de la inteligencia Artificial para suplantar la identidad de otra persona está teniendo una gran incidencia en los últimos años, por lo que se requiere

medidas efectivas para contrarrestar esta problemática, así como del análisis amplio del marco legal en relación a la suplantación de identidad y otros delitos informáticos que van de la mano.

Por último, se reconoce que los delitos informáticos traspasan fronteras internacionales, por lo que se requiere de la cooperación entre países para combatir las consecuencias y daños hacia la víctima y su patrimonio.

## 7. Recomendaciones / propuestas

### 7.1. Recomendaciones

Para evitar que ocurran estas situaciones tenemos algunas recomendaciones

1. Evitar ingresar su información personal, como contraseñas, fechas de nacimiento, etc., en cualquier sitio web porque se puede caer en el phishing, y mediante este, se puede cometer la suplantación de identidad porque la persona puede recolectar toda la información a través de esta modalidad y así, puede hacerse pasar por esta persona, para cometer el delito de suplantación de identidad
2. Tener actualizados los software y parches de seguridad de nuestros dispositivos electrónicos, para evitar que roben nuestros datos privados.
3. No almacenar contraseñas en computadores de acceso público, evitar compartir nuestras contraseñas a otras personas, estar pendientes de que nadie vea nuestra contraseña y usar contraseñas seguras, así podremos evitar la suplantación de identidad.

### 7.2. Propuesta

Como parte de la investigación realizada, tenemos como propuesta un nuevo tipo penal o la reforma del articulado 212 del Código Orgánico Integral Penal, donde se tipifiquen las nuevas formas, maneras y técnicas en base a la tecnología para la suplantación de identidad de una persona; específicamente con el uso fraudulento de la Inteligencia Artificial, como el Deepfake u otros programas que manipulen fotografías, videos y voces. Así mismo estableciendo grados de responsabilidad para las personas que participen dentro de este tipo penal que ayude, colabore, preste o omita alguna acción para llevar a cabo este delito, mas aun quienes son tenedores

de datos personales y están encargados de guardarlos y no usarlos sin autorización del titular.

**Art. 212 a. Suplantación de identidad usando inteligencia artificial.** La persona que suplante la identidad de otra, valiéndose del uso de cualquier software de inteligencia artificial para obtener un beneficio propio o para un tercero, en perjuicio de otra persona, será sancionada con pena privativa de libertad de 3 a 5 años, y si el delito es cometido por aquellos considerados como tenedores de la información personal, la pena privativa de libertad será de 5 a 7 años, con las prohibición de no volver a trabajar en cualquier lugar que se encargue de recopilar y guardar datos personales y con una multa de diez salario básico unificados.

## 8. Bibliografía


Acosta, M. G., Benavides, M. M., & García, N. P. (01 de 01 de 2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89), 351. Obtenido de https://produccioncientificaluz.org/index.php/rvg/article/view/31534/32619

Aparicio-Izurieta, V. V. (15 de 02 de 2022). Delitos informáticos en Ecuador según el COIP: unanálisis documental. *Sapienza: International Journal of Interdisciplinary Studies, vol.3*(n.1 ). doi:10.51798

Barrientos Báez , A., Piñeiro Otero, T., Porto Renó , D. (21 de Mayo de 2024). Imágenes falsas, efectos reales. Deepfakes como manifestaciones de la violencia política de género. *Revista Latina de Comunicación Social*(82), 1 - 29. Obtenido de https://nuevaepoca.revistalatinacs.org/index.php/revista/article/view/2278/4956

Diaz Basurto, I. J., Ojeda Sotomayor, P. M., Cajas Parraga, C. M., & Cabrera Ripalda, E. P. (Noviembre de 2023). DESAFIOS LEGALES EN ECUADOR FRENTE A LOS DELITOS INFORMÁTICOS, IMPORTANCIA DE SU PREVENCIÓN. *UNIVERSIDAD Y SOCIEDAD. Revista cientifica de la Universidad de Cienfuegos, 15*(6), 746-754. Obtenido de https://rus.ucf.edu.cu/index.php/rus/article/view/4195/4102

Ecuador, A. N. (2008). Constitucion de la Republica del Ecuador . *CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008*. Ecuador.

Ecuador, A. N. (17 de Feb. de 2021). Codigo Organico Integral Penal, COIP. Quito, Ecuador.

Ecuador, A. N. (26 de mayo de 2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. Ecuadro : Registro Oficial .

Ecuador, R. d. (s.f.). *Ministerio de Educación* . Obtenido de Ministerio de Educación : https://recursos.educacion.gob.ec/red/hacking/

Endara-Chamorro , R. E., Espinoza-Jiménez, J. S., López-Fuel, E. R., & Santander Moreno, J. J. (01 de febrero de 2024). Análisis jurídico del deepfake en relación a la suplantación de identidad, Ecuador. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas, 9*(1), 240 - 250. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9545770

Estado, F. G. (2024). *Registros de noticias del delito en el Sistema SIAF del Delito de Suplantación de Identidad.* noticias del delito , Fiscalia General del Estado , Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE , Ecuador.

Hermosilla, O. M. (2023). INTELIGENCIA ARTIFICIAL, BIDGATA Y DERECHO A LA PROTECCIÓN DE DATOS DE LAS PERSONAS TRABAJADORAS. *Revista de Estudios Jurídico Laborales y de Seguridad Social*, 90-117. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8954369

Institute, L. (2024). *Lisa Institute* . Obtenido de Lisa Institute : https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

Juan José Camargo-Vega, J. F.-O.-A. (2015). Conociendo Big Data. *Revista Facultad de Ingeniería* , 63-77.

Kemp, S. (26 de Enero de 2022). *We are Social* . Obtenido de We Are Social: https://wearesocial.com/es/blog/2022/01/digital-report-2022-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/

Loján Alvarado, H. P., & Cárdenas Villavicencio, O. E. (Enero-Febrero de 2024). REGULACIÓN DEL MANEJO DE LA INTELIGENCIA ARTIFICIAL, CONSECUENCIAS Y DAÑOS A LA SOCIEDAD POR SU MAL USO. *Ciencia Latina Revista Cientifica Multidisciplinar, 8*(1), 1966-1978. Obtenido de https://ciencialatina.org/index.php/cienciala/article/view/9596/14194

Macías-Lara, R. A., Boné Andrade, M. F., Quiñonez Angulo, F., Mendoza Loor, J. J., Estupiñan Troya, G., & Rodríguez Vizuete, J. D. (03 de 01 de

2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Sapienza International Journal of Interdisciplinary Studies., Vol. 3*(N. 2), 231 - 242. doi:10.51798

Mariano Díaz, R. (Noviembre de 2020). La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. *(16)*, 18. (CEPAL), Comisión Económica para América Latina y el Caribe;. Obtenido de CEPAL: https://repositorio.cepal.org/server/api/core/bitstreams/6727e17b-6ebc-4544-b8cf-5f859a45fa28/content

Mayer Lux, L., & Calderon , G. O. (2020). El delito de fraude informático: Concepto y delimitación. *REVISTA CHILENA DE DERECHO Y TECNOLOGIA*, 151-184.

Mok, S. C. (2020). Privacidad y protección de datos: un análisis de legislación comparada. *Diálogos Revista Electrónica de Historia*, 111-152.

Obando I, C., & Vásquez V, M. (10 de Enero de 2022). Seguridad a nivel de enlace de datos en el modelo de interconexión de sistemas abiertos (OSI). *Ingente Americana, 2*(2), 71-78. Obtenido de https://publicaciones.americana.edu.co/index.php/inam/article/view/405/632

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (Enero-Febrero de 2021). ANÁLISIS CONCEPTUAL DEL DELITO INFORMÁTICO EN ECUADOR. *Revista pedagogica de la Universidad de Cienfuegos, vol. 17*(n. 78), 345-350. Recuperado el 04 de Julio de 2024, de Conrado: http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext

Sevilla Robles, M. A. (26 de 03 de 2023). *Resumen sobre Internet.* Obtenido de Dspace: http://148.202.167.116:8080/xmlui/handle/123456789/3088?show=full

States, O. o., & Europa, C. d. (03 de NOVIEMBRE de 2001). Convenio sobre la Ciberdelincuencia. *Convenio de Budapest*. BUDAPEST. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Toala Indio, Y. (2021). Delitos informáticos frecuentes en el Ecuador: casos de estudio. *Repositorio Institucional de la Universidad Politécnica Salesiana*. Recuperado el 05 de julio de 2024, de https://dspace.ups.edu.ec/bitstream/123456789/20942/1/UPS-GT003389.pdf

*Universidad Isabel I.* (13 de 02 de 2023). Obtenido de Universidad Isabel I: https://www.ui1.es/blog-ui1/sistemas-informaticos-si-que-son-caracteristicas-y-tipos.

https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f36afdf-40eb-4cba-a38f-5827107779a9/content

Macías-Lara, R. A.., Boné Andrade, M. F. ., Quiñonez Angulo, F. ., Mendoza Loor, J. J., Estupiñan-Troya, G. ., & Rodríguez Vizuete, J. D. . (2022). Frequent cases, criminalization and prevention of computer crimes in Ecuador: a brief systematic review. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2), 231–243. https://doi.org/10.51798/sijis.v3i2.324

Ecuavisa . (2023, Diciembre 28). *ECUAVISA*. From ECUAVISA: https://www.ecuavisa.com/noticias/seguridad/mafias-coyoteros-inteligencia-artificial-estafar-familias-migrantes-DC6545041

Ecuavisa. (2024, Julio 09). *ECUAVISA*. From ECUAVISA: https://www.ecuavisa.com/noticias/seguridad/imagenes-o-audios-manipulados-con-inteligencia-artificial-de-los-presentadores-de-televistazo-circulan-en-redes-YB7641320

# 9. Anexos

## 9.1. Entrevistas

***Entrevista 1***

**Nombre:** Juan Martínez Loor.

**Profesión:** Doctor en Jurisprudencia (Abogado en libre ejercicio profesional)

**1.- Desde su experticia profesional ¿que conoce usted sobre el delito de suplantación de identidad?**

De conformidad con lo establecido en el Art. 212 del Código Orgánico Integral Penal, el delito de suplantación de identidad comprende a *"la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona"* y la sanción es una pena privativa de libertad de uno a tres años, es decir que se configura cuando una persona se hace pasar por otra, utilizando

su nombre, documentos o cualquier otro dato personal con la intención de cometer un fraude, obtener un beneficio o causar un daño.

**2. ¿Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**

Sí, considero que el delito de suplantación de identidad puede ser cometido utilizando como medio del delito la inteligencia artificial, toda vez que conocemos que esta tecnología permite crear simulaciones muy realistas de personas, mediante imágenes, voces y más datos personales.

**3.- ¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

El uso fraudulento de la inteligencia artificial puede servir como delito medio para otros delitos fines más allá de la suplantación de identidad, entre ellas: fraudes financieros, extorsión, espionaje, estafa, difusión de información falsa, ataque de redes informáticas, manipulación de datos, etc.

**4.- Desde su experticia profesional ¿cómo cree que se vulneran los datos personales usando la inteligencia artificial?**

Las vulneraciones podrían cometerse mediante el acceso no autorizado a bases de datos, la extracción y uso indebido de información personal, perfiles falsos, violaciones de la intimidad y la privacidad, difusión de imágenes propias o de su círculo familiar.

**5.- ¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**

El solo hecho de ser tenedor de información personal no debería ser causal para responsabilizar a alguien de un delito, pero sí debe establecerse controles y declaraciones legales de someterse a responsabilidad ante un uso indebido de esos datos que le han sido confiados. Para ello en el Ecuador ya existe la ***LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*** la cual asegura que las entidades que recopilan, almacenan y procesan datos personales implementen medidas adecuadas de seguridad y privacidad.

*Entrevista 2*

**Nombre:** Xavier Andrés Ronquillo Carchi.

**Profesión:** Abogado.

**Preguntas para la entrevista**

1. **Desde su experticia profesional ¿que conoce usted sobre el delito de suplantación de identidad?**

Si conozco, en tal virtud este se encuentra entre los delitos en contra el derecho a la identidad, dentro del cual se establece que la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, tendrá una sanción de pena privativa de libertad de uno a tres años.

**Ejemplo:** Actualmente existen un gran número de denuncias por el delito de suplantación de identidad, dentro de las cuales personas desconocidas, muchas veces manejadas por redes internacionales, utilizan información personal que se encuentra dentro de nuestras redes sociales, para el cometimiento de este delito, que, en su mayoría, piden dinero, indicando hechos que no son reales.

2. ¿**Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**

Considero que sí, en tal virtud de que dentro del mismo Art. 212 del COIP, establece de manera expresa que la persona que de **cualquier forma suplante la identidad de otra para obtener un beneficio**, es decir, podría considerarse que, al utilizar el uso de inteligencia artificial, que es una herramienta nueva y que lamentablemente puede ser utilizada para el cometimiento de este y cualquier otro delito.

3. **¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

Pues considero que sí, puede generar otras conductas que no se encuentran descritas en la normativa penal vigente, ya que la conducta del ser humano es cambiante, y al pasar del tiempo se van generando otros tipos de problemáticas que luego tienen que ser consideradas y reprimidas en la ley.

4. **Desde su experticia profesional ¿cómo cree que se vulneran los datos personales usando la inteligencia artificial?**

Es muy importante señalar que nuestra información personal en la actualidad lamentablemente se encuentra muy expuesta, tanto en nuestras redes sociales, como la que uno entrega a las entidades públicas o privadas, que de manera fraudulenta las grandes mafias compran dicha información, convirtiéndonos en presa fácil para el cometimiento de algún delito.

5. **¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**

Efectivamente, sería conveniente establecer no solos grados de responsabilidad penales tanto para las personas naturales y jurídicas que manejen información personal, sino que también debería existir en algún momento una reforma al COIP, que establezca parámetros para su buen uso y de ser posible, que obliguen a las mismas a un buen uso de dicha información.

***Entrevista 3***

**Nombre: Simón González Castro**

**Profesión: Abogado de los Tribunales del Ecuador**

**Preguntas para la entrevista**

1. **¿Desde su experticia profesional que conoce usted sobre el delito de suplantación de identidad?**

   La suplantación de identidad es una forma en la cual una persona adopta la identidad de otra con la finalidad de beneficiarse y hacer pasar por ella perjudicando el nombre de la persona a quien se le ha tomado su identidad. Lo cual constituye a un delito penado. El delito de suplantación de identidad está tipificado en el artículo 246 del código órgano orgánico integral penal (COIP) en el Ecuador

2. **¿Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**

   Sí, es posible que exista el delito de suplantación de identidad mediante el uso de inteligencia artificial. La tecnología de inteligencia artificial está avanzando

rápidamente y puede ser utilizada para crear perfiles falsos o engañosos en línea, tomándose la identidad de una persona de buen nombre y comportamiento para cometer un sin número de delitos. Además, la inteligencia artificial también puede ser utilizada para crear videos o audios falsos que pueden ser utilizados para engañar a las personas y hacer que crean que están hablando con alguien que en realidad no es esa persona. Por lo tanto, es importante que se tomen medidas para prevenir y sancionar este tipo de delitos.

3. **¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

   Sí, el uso fraudulento de la inteligencia artificial puede generar otras conductas delictivas. Por ejemplo, el uso de la inteligencia artificial para crear perfiles falsos en redes sociales o sitios web de citas puede ser utilizado para cometer delitos como el acoso, la extorsión, estafas y otras más. Además, el uso de la inteligencia artificial para crear videos o audios falsos puede ser utilizado para cometer delitos como la difamación, la manipulación de pruebas o la intimidación. Es importante que se tomen medidas para prevenir y sancionar este tipo de delitos, y que se fomente el uso responsable y ético de la inteligencia artificial.

4. **¿Desde su experticia profesional como cree que se vulneran los datos personales usando la inteligencia artificial?**

   Si bien es cierto la inteligencia artificial es una herramienta muy poderosa en las manos correctas, pues también se vulneran los datos personales de varias maneras, entre ellas:

   1. Robo de identidad,
   2. Ataques de phishing
   3. Espionaje
   4. Robo de contraseñas
   5. Hackeos de cuentas

Las personas deben tomar medidas para proteger su información personal, no compartir información personal en línea y utilizar software de seguridad en sus dispositivos. Además, es importante que las empresas y organizaciones también tomen medidas para proteger la información personal de sus clientes y empleados. Muchas veces estas mismas filtran información.

5. **¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**

   Claro, considero que se deben establecer grados de responsabilidad legal a los tenedores de la información personal. Las empresas y organizaciones que recopilan y almacenan información personal de sus clientes y empleados tienen la responsabilidad de proteger esa información y garantizar su privacidad y seguridad. Se produce una violación de datos o se da un mal uso de la información personal.

   Deben establecerse leyes y regulaciones claras que definan las responsabilidades y obligaciones de los tenedores de información personal, y que se establezcan sanciones adecuadas para aquellos que no cumplan con estas obligaciones. Además, es importante que se fomente una cultura de privacidad y seguridad de datos en todas las empresas y organizaciones, y que se promueva la educación y concientización de los usuarios sobre la importancia de proteger su información personal.

***Entrevista 4***

**Nombre:** José Orejuela**.**

**Profesión:** Abogado (defensor público)

**Preguntas para la entrevista**

1. **¿Desde su experticia profesional que conoce usted sobre el delito de suplantación de identidad?**

   Sobre los delitos de suplantación de identidad en mi experiencia personal dentro del ámbito donde laboro he tenido algunos casos de suplantación de identidad, donde claramente este caso se determine de acuerdo lo que establece el art. 212 del COIP. Existe suplantación de identidad y se ha dado en muchos casos por ejemplo en las elecciones cuando hay personas que en este caso tiene algún problema judicial, entonces prefieren mandar a otra persona para que sufrague por ellos y así no tener este tipo de inconvenientes, es ahí donde se genera o se configura el delito de suplantación de identidad;

estos son los casos más comunes que han existido dentro de mi ámbito profesional.

2. **¿Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**

   Haber, en este caso debido a todas las tecnologías que se están dando dentro de nuestro sistema ecuatoriano y creo que, a nivel mundial, se está dando este tipo de suplantación de identidad porque hemos visto muchas tecnologías aplicadas para que personas que no existen puedan hablar, puedan bailar, puedan hacer sin número de situaciones. También no solamente para generar algún tipo de humor sino, también para cometer delitos, entonces, si se está generando este tipo de delitos con Inteligencia Artificial en estos últimos días.

3. **¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

   Obvio, en este caso como lo manifesté anteriormente no se está solo dando este tipo de inteligencia artificial para crear contenido más que todo en las redes sociales en base a generar humor, sino, también generando otro tipo de conducta para cometer delitos, incluso está generando otro tipo de delitos para pedir dinero, exigir información de cuentas y en este caso también cometer fraude dentro de las cuentas de las personas que emite sus datos personales dentro de las redes sociales. Entonces si se está utilizando este tipo de inteligencia artificial no solamente generar humor sino para cometer delitos, están generando otro tipo de conducta ilícita para cometer algún tipo de delito.

4. **¿Desde su experticia profesional como cree que se vulneran los datos personales usando la inteligencia artificial?**

   Bueno los datos personales recordemos que la mayoría de todos los seres humanos tenemos y nos exigen en nuestras redes sociales todos los datos personales y para cualquier cuenta o medio tecnológico y hasta para hacer una compra vía online nos exigen nuestros datos personales y esto conlleva a que puedan ser de uso público para cometer este tipo de delito. Recordemos también que, en estos casos debido a este tipo de delitos por medio de IA, se está generando el acceso no solamente a las cuentas sino a los datos personales de cada persona, incluso fotos.

5. **¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**

   Claro, desde mi punto de vista obvio se debe generar un grado de responsabilidad, ¿pero como lo pueden hacer?, ¿cómo lo van hacer?, primero no está tipificados segundo va ser muy difícil en este caso establecer la responsabilidad cuando sabemos que nuestras redes sociales son públicas lo que significa que no se puede tener una privacidad en este caso y va ser muy difícil exigir una responsabilidad. En conclusión, son dos puntos importantes a recalcar, el primero no está tipificada la responsabilidad legal y el segundo existen dudas en cuanto a la responsabilidad, precisamente porque es pública la información que está en redes sociales.

***Entrevista 5.***

**Nombre:** Francisco Moreira.
**Profesión:** Abogado (defensor público)

**Preguntas para la entrevista**

1. **¿Desde su experticia profesional que conoce usted sobre el delito de suplantación de identidad?**

   Efectivamente el delito de suplantación de identidad está tipificado en el COIP art. 212 como la persona que suplante de una u otra manera la identidad de otra. En cuestiones de suplantación puede haber una falsifica ion de documentos de identificación(cedula), documentos públicos para realizar cualquier trámite o a la vez usufructuar esa identificación y obtener un beneficio.

2. **¿Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**

   Con la nueva tecnología si existe una suplantación de identidad mediante inteligencia artificial, lastimosamente en el COIP no está tipificado un modus operandi nuevo, no hay una reforma a pesar de que ahora último hubo una reforma del código y no se trató específicamente de eso; si existe muchos casos que se encuentran surgiendo y que incluso está oficializándose ese tipo

de pruebas y no tenemos delitos en la materia, expertos que analicen ese tipo de pruebas: si son producidas con IA, sin son editadas, etc. Pienso que ahí, en ese sentido el sistema de justicia necesita estabilizarse. La reforma debe ir acompañada de personas que conozcan la materia, porque si vamos a introducir un prueba, que, puede ser sujeta a un análisis y no tenemos la persona que analice de la manera correcta esa prueba que es forzada con IA, lógicamente no va a tener un éxito la reforma, es un engranaje que se debe tener en cuenta desde el fiscal que tiene que estar especializado y tener conocimientos en ese tipo de delitos y el eje investigativo: Los agentes de la policía judicial o peritos especializados en esa rama y acreditados por el consejo de la judicatura, que sepan aplicar software o programas a fin de verificar si la prueba es original o no.

3. **¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

   Claro, precisamente lo que le decía anteriormente no solamente hay suplantación de identidad, hay también falsificación de documentos, de instrumentos públicos; todo lo genera la tecnología en todo caso, más que otras conductas yo creo que la suplantación de identidad tendría que ampliarse no solamente a la suplantación de identidad de falsificar un documento público sino a la suplantación de identidad por videos, que tiene que estar inmerso en el mismo tipo penal. De una u otra manera, sigue siendo una suplantación de identidad porque está utilizando la imagen de otra persona con fines de cometer algún acto ilícito, pero no creo que genero otras conductas, yo creo que esa conducta esta subsumida en el mismo delito de suplantación de identidad.

4. **¿Desde su experticia profesional como cree que se vulneran los datos personales usando la inteligencia artificial?**

   Lastimosamente ahí se debería crear una ley que proteja los datos personales, si hay, reformarla a fin de que sean restringidos los datos, para proporcional mas seguridad. Mira, tenemos incluso a veces problemas con los bancos, hay compras internacionales de bases de datos originadas de los bancos y así existen delitos cibernéticos, usurpado información personal o tomando

información personal que no es tan personal, sino pública y que las instituciones encargadas de guardar esa información no gestionan o respaldan correctamente de lo que es una información personal, entonces ahí, tendría que hacerse una investigación o reformar la ley a fines de que existan un ente de control eficiente que supervise el uso de datos personales en manos de empresas públicas y privadas, y que a veces son mal utilizados.

5. **¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**
   Por supuesto que debe haber una responsabilidad en ese sentido, no solamente regular el uso sino también hacer ver quien es la persona que facilita esa información para cometer los actos ilícitos. Entonces estaría un grado de participación la persona que entregue una información personal a otra con el fin de cometer un acto ilícito. O sea, si tiene responsabilidad quien otorgue una información personal, si hay un grado de participación. Pero debería haber una reforma de la ley con respecto al uso de la información personal.

***Entrevista 6***

**Nombre: Luis Fernando Plúas**

**Profesión: Abogado**

**Preguntas para la entrevista**

1. **¿Desde su experticia profesional que conoce usted sobre el delito de suplantación de identidad?**
   Si, la suplantación de identidad, es un delito que consiste en el cual una persona se hace pasar por otra para obtener un beneficio que no puede conseguirlo con su verdadera identidad, inclusive esto es un grave riesgo en el cual pueden acceder a información sensible, confidencial para cometer otros delitos.
2. **¿Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**
   Si, hoy en día con los nuevos avances tecnológicos e inteligencias artificiales los delincuentes han usado y optado por cometer delitos a través de

plataformas digitales, creando perfiles, usuarios, clonación de tarjetas perjudicando a la verdadera persona que tiene su identidad.

3. **¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

   El mal uso de cualquier herramienta tecnológica sin duda genera otras conductas, como, por ejemplo, la misma suplantación de identidad, estafas, y conductas continuadas que generan en el transcurso del tiempo redes delictivas que agrupan personas para cometer actividades delictivas

4. **¿Desde su experticia profesional como cree que se vulneran los datos personales usando la inteligencia artificial?**

   Primero hay que entender que la inteligencia artificial se enfoca principalmente en el procesamiento de datos y tomar decisiones basadas a través del aprendizaje automático, el razonamiento y la percepción, el mal uso conllevaría a otras conductas inusuales, pues toda plataforma tecnológica ha llegado para facilitarnos la vida y hacerla más sencilla.

5. **¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**

   La responsabilidad penal radica en aquella persona que teniendo voluntad y conciencia comete o cometen delitos, pero si es importante que, las personas sean más diligentes y cuidadosas con el uso de su información personal, pues con el robo de pertenencias y de datos, el delito de suplantación de identidad está en auge, y esto es un desafío grande que las autoridades deben contrarrestar.

***Entrevista 7***

**Nombre: Betty Pilar Mejía León**

**Profesión: Abogada**

**Preguntas para la entrevista**

1. **¿Desde su experticia profesional que conoce usted sobre el delito de suplantación de identidad?**

   La suplantación de identidad es una actividad delictiva regulada en nuestro ordenamiento jurídico tipificado en el articulo 212 del Código Orgánico Integral Penal (COIP) que la define como: “la persona que de cualquier forma suplante la

identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años" Es decir, la suplantación de identidad consiste en utilizar datos personales de una persona sin el consentimiento de ésta, con la finalidad de obtener un beneficio y en perjuicio de la víctima y de un tercero, evidenciando que si utiliza la identidad real no podría conseguir el beneficio.

2. **¿Considera usted que existe el delito de suplantación de identidad mediante el uso de inteligencia artificial?**

En la actualidad la utilización de la inteligencia artificial es cada vez es más riesgoso pues al tener acceso a información de una persona, esta puede ser robada, pues constantemente colgamos fotos, videos, gestos, e información que fácilmente puede ser modificada, alterada por la inteligencia artificial, obteniéndose perfiles falsos, que puede confundir y engañar a los que conocen e inclusive a instituciones que tratamos o donde tengamos nuestros intereses, que una vez obtenida y utilizada se puede inclusive obtener beneficios patrimoniales, económicos, información confidencial, Etc.

**¿Cree usted que el uso fraudulento de la inteligencia artificial genera otras conductas?**

Si, pues la utilización inadecuada genera conductas delictivas, tales como:
**Ciberdelincuentes, estafas y fraudes.**

3. **¿Desde su experticia profesional como cree que se vulneran los datos personales usando la inteligencia artificial?**

   Constantemente compartimos y dejamos información personal en los sitios web que visitamos e inclusive muchas veces guardamos claves de acceso, preguntas de seguridad, datos de las huellas digitales en los portales que visitamos para hacer algún trámite o adquirir un servicio o bien. Información que es utilizada por los delincuentes expertos en la obtención de información o hacker.

4. **¿Considera usted que se deben establecer grados de responsabilidad legal a los tenedores de la información personal?**

   Claro que si, al entregarse información de una persona a una tercera persona para que este la utilice de manera adecuada y en muchos de los casos se convierta en custodio de esa información, se debe haber comprometido en ser

responsable del manejo, distribución y de difundir de los datos personales de su mandatario; pues el tenedor descuida de esta información causa un perjuicio inminente a la víctima. Al nivel de empresa se debe capacitar constantemente al empleado que maneja la información de sus jefes ya que a través de clonación de voz fácilmente puede causar un perjuicio inmenso a la empresa.

### 9.2. Informe estadístico respecto al delito de suplantación de identidad por parte de la Fiscalía General del Estado

## DIRECCIÓN DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN

### Registros de noticias del delito en el Sistema SIAF del Delito de Suplantación de Identidad

- Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE
- Fecha de corte: 31/5/2024
- Periodo de análisis: (01/01/2019) - (31/05/2024)
- Unidad de Análisis: Noticias de delito

**Tabla 1 Noticias del delito de suplantación de identidad a nivel nacional registradas en el Sistema SIAF**

| PROVINCIA | CONSUMADO | | | | | | TENTATIVA | | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | |
| AZUAY | 176 | 154 | 263 | 146 | 137 | 44 | 1 | 1 | | 1 | | 1 | 924 |
| BOLIVAR | 18 | 24 | 19 | 22 | 40 | 13 | | | | | | | 136 |
| CANAR | 29 | 15 | 29 | 35 | 30 | 16 | | | | | | | 154 |
| CARCHI | 35 | 26 | 26 | 26 | 20 | 9 | | | 1 | 1 | | | 144 |
| CHIMBORAZO | 46 | 47 | 60 | 51 | 54 | 35 | 1 | | | | 1 | | 295 |
| COTOPAXI | 62 | 48 | 54 | 52 | 82 | 24 | | | 1 | | 1 | | 324 |
| EL ORO | 182 | 162 | 236 | 232 | 184 | 113 | | 3 | 2 | | | 4 | 1.118 |
| ESMERALDAS | 53 | 47 | 66 | 91 | 84 | 41 | 1 | | | | | | 383 |
| GALAPAGOS | 11 | 7 | 10 | 4 | 19 | 6 | 1 | | | | | 1 | 59 |
| GUAYAS | 2.129 | 1.448 | 2.076 | 2.116 | 2.363 | 943 | 13 | 10 | 7 | 10 | 11 | 4 | 11.130 |
| IMBABURA | 114 | 79 | 143 | 162 | 168 | 83 | 1 | 2 | | | | | 752 |
| LOJA | 67 | 81 | 133 | 141 | 100 | 53 | | 1 | 1 | | 1 | | 578 |
| LOS RIOS | 100 | 54 | 108 | 130 | 129 | 67 | 2 | | 1 | | | 2 | 593 |
| MANABI | 240 | 171 | 284 | 284 | 281 | 146 | 2 | 1 | | 1 | 1 | | 1.411 |
| MORONA SANTIAGO | 18 | 10 | 15 | 18 | 25 | 4 | | | 1 | | | 1 | 92 |
| NAPO | 16 | 7 | 28 | 25 | 24 | 9 | | | | 1 | | | 110 |
| ORELLANA | 22 | 22 | 25 | 37 | 44 | 17 | | 1 | | | | | 168 |
| PASTAZA | 16 | 8 | 18 | 13 | 16 | 6 | | | | 1 | | | 78 |
| PICHINCHA | 950 | 1.222 | 2.125 | 1.970 | 2.259 | 810 | 8 | 8 | 22 | 6 | 8 | 7 | 9.395 |
| SANTA ELENA | 28 | 35 | 60 | 66 | 71 | 42 | | 1 | | | 2 | | 305 |
| SANTO DOMINGO DE LOS TSACHILAS | 52 | 55 | 73 | 106 | 130 | 55 | 1 | | 1 | | | | 473 |
| SUCUMBIOS | 20 | 27 | 42 | 47 | 52 | 11 | | | | | 1 | | 200 |
| TUNGURAHUA | 157 | 119 | 129 | 92 | 116 | 32 | | | | 1 | | | 646 |
| ZAMORA CHINCHIPE | 10 | 13 | 12 | 8 | 17 | 11 | | | | | | | 71 |
| **Total general** | **4.551** | **3.881** | **6.034** | **5.874** | **6.445** | **2.590** | **31** | **28** | **37** | **22** | **26** | **20** | **29.539** |

**Tabla 2 Noticias del delito de suplantación de identidad a de la Provincia del Guayas registradas en el Sistema SIAF**

| Cantón | CONSUMADO | | | | | | TENTATIVA | | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | |
| ALFREDO BAQUERIZO MORENO ( JUJAN ) | | | | 1 | | 2 | | | | | | | 3 |
| BALAO | | 1 | 1 | | | 5 | | | | | | | 7 |
| BALZAR | 8 | 5 | 3 | 6 | 12 | 1 | | | | | | | 35 |
| COLIMES | 1 | | | | | 1 | | | | | | | 2 |
| DAULE | 35 | 46 | 53 | 58 | 74 | 25 | | | | | | | 291 |
| DURAN | 107 | 63 | 89 | 108 | 80 | 39 | | | | 1 | 1 | 2 | 490 |
| EL EMPALME | 48 | 17 | 18 | 15 | 20 | 8 | | | | | | | 126 |
| EL TRIUNFO | 10 | 9 | 5 | 12 | 12 | 4 | | | | | | | 52 |
| GENERAL ANTONIO ELIZALDE (BUCAY) | 2 | | 1 | | 4 | 1 | | | | | | | 8 |
| GUAYAQUIL | 1.825 | 1.212 | 1.776 | 1.775 | 1.992 | 750 | 13 | 9 | 7 | 7 | 10 | 2 | 9.378 |
| LOMAS DE SARGENTILLO | 1 | | | | 2 | | | | | | | | 3 |
| MILAGRO | 33 | 42 | 32 | 42 | 35 | 24 | | | | 1 | | | 209 |
| NARANJAL | 6 | 8 | 14 | 17 | 17 | 16 | | | | | | | 78 |
| NARANJITO | 3 | 1 | 12 | 3 | 6 | 7 | | | | | | | 32 |
| NOBOL | 3 | 1 | 2 | 4 | 2 | 1 | | | | | | | 13 |
| PALESTINA | 1 | | | 1 | 28 | 5 | | | | | | | 35 |
| PEDRO CARBO | 6 | 3 | 8 | 10 | 3 | 2 | | | | | | | 32 |
| PLAYAS | 13 | 14 | 12 | 15 | 25 | 33 | | | | | | | 112 |
| SALITRE | 3 | 1 | 3 | 4 | 3 | 3 | | | | | | | 17 |
| SAMBORONDON | 15 | 17 | 23 | 31 | 26 | 8 | | 1 | | 1 | | | 122 |
| SAN JACINTO DE YAGUACHI | 6 | 7 | 18 | 7 | 11 | 5 | | | | | | | 54 |
| SANTA LUCIA | 2 | 1 | 5 | 3 | 7 | 2 | | | | | | | 20 |
| SIMON BOLIVAR | 1 | | 1 | 4 | 4 | 1 | | | | | | | 11 |
| **Total general** | **2.129** | **1.448** | **2.076** | **2.116** | **2.363** | **943** | **13** | **10** | **7** | **10** | **11** | **4** | **11.130** |

**DIRECCIÓN DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN**

## Informe Estadístico

| | |
|---|---|
| **Fecha de suscripción de la solicitud:** | 31/5/2024 |
| **Número de documento de ingreso de solicitud:** | Ticket# 2024053122000865 |
| **Nombre y apellido de la persona solicitante:** | Karla Cedeño |
| **Cédula de la persona solicitante:** | |
| **Correo electrónico de la persona solicitante:** | KarlaCedeno.02@hotmail.com |
| **Tipo del solicitante:** | 1 |
| **Fecha ingreso a la Dirección:** | 31/5/2024 |
| **Fecha de reasignación al analista:** | 4/6/2024 |
| **Fecha de respuesta:** | 5/6/2024 |
| **Tipo de medio de notificación:** | Mesa de ayuda |
| **Número de documento de ingreso de solicitud (Memorando, Oficio):** | Ticket# 2024053122000865 |
| **Detalle de la información requerida:** | Estadísticas del Noticias del delito de Suplantación de Identidad de los últimos 5 años a nivel nacional y provincia de Guayas y Cantón Guayaquil |
| **Tipos penales:** | Suplantación de Identidad |

**Procedimiento de extracción de información:**

| | |
|---|---|
| · **Fuente**: | Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE |
| · **Fecha de corte:** | 31/5/2024 |
| · **Periodo de análisis:** | (01/01/2019) - (31/05/2024) |
| · **Unidad de Análisis:** | Noticias de delito |

· **Consideraciones:**

1. Se cuantifica el total de Noticia del Delito (NDD) registradas en el Sistema Integrado de Actuaciones Fiscales (SIAF). Se contabilizan también las NDD que tienen dos o más registros, que corresponden a un mismo hecho delictivo y fueron asignadas a diferentes Fiscalías Especializadas debido a la naturaleza de la investigación.
2. Consumado / tentativa

| | |
|---|---|
| **Elaboración:** | Valeria Mariño |
| **Revisión y aprobación:** | Alex Tupiza |
| **Fecha de revisión y aprobación:** | 5/6/2024 |

Se informa al peticionario que según:

**La Constitución de la República del Ecuador:**

Artículo 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

**La Ley Orgánica de Transparencia y Acceso a la Información Pública**

Artículo 1.- Principio de Publicidad de la Información Pública.- El acceso a la información pública es un derecho de las personas que garantiza el Estado.

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema material de la información tengan participación del Estado o sean concesionaros de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.

**La Dirección de Estadística y Sistemas de Información atenderá éste pedido durante los 10 días siguientes a la recepción del mismo o, a más tardar, dentro del plazo establecido en el Artículo 9 de la Ley Orgánica de Transparencia y Acceso a la Información Pública – LOTAIP**

**De conformidad con el Código Orgánico Integral Penal**

Artículo 472, no podrá circular libremente la siguiente información:

1) Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley.

2) La información acerca de datos de carácter personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la ley o por el juzgados.

3) La información producida por la o fiscal en el marco de una investigación previa y aquella original en la orden judicial relacionada con las técnicas especiales de investigación.

4) La información acerca de niñas, niños y adolescentes que viole sus derechos según lo establecidos en el Código Orgánico de la Niñez y Adolescencia y la Constitución.

5) La información calificada por los organismos que conforman el Sistema nacional de inteligencia.

Artículo 584

6) Las actuaciones de la Fiscalía, de la o el juzgador, del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses, la Policía Nacional, y de otras instituciones que intervienen en la investigación previa, se mantendrán en reserva, sin perjuicio del derecho de la víctima y de las personas a las cuales se investigan y sus abogados a tener acceso inmediato, efectivo y suficiente a las investigaciones, cuando lo soliciten.

7) Cuando el personal de las instituciones mencionadas, los peritos, traductores, interpretes, que han intervenido en estas actuaciones, divulguen o pongan de cualquier modo en peligro el éxito de la investigación o las difundan, atentando contra el honor y al buen nombre de las personas en general, serán sancionadas conforme con lo previsto en este Código.

**Ley Orgánica de Comunicación**

*Con base en al principio de responsabilidad ulterior contenido en el Artículo 19 de la Ley Orgánica de Comunicación, que establece que la responsabilidad ulterior es la obligación que tiene toda persona de asumir las consecuencias administrativas posteriores a difundir contenidos que lesiones los derechos establecidos en la Constitución y en particular los derechos de la comunicación y la seguridad pública del Estado, a través de los medios de comunicación, sin perjuicio de las acciones civiles penales o de cualquier otra índole a las que haya lugar; la FGE requiere al peticionario utilizar la información proporcionada solo para los fines específicamente establecidos en la solicitud, así como, hacer uso responsable de la misma.