UNIVERSIDAD CES / FACULTAD DE DERECHO

ARTÍCULO DE REFLEXIÓN

Suplantación de Identidad: Una Mirada desde el Derecho Comparado

Identity Theft at a Global Level: A Perspective from Comparative Law

Yeffrin Sebastián Naranjo Hincapie
Estudiante del pregrado de Derecho de la Universidad CES – Medellín - Colombia

Resumen

El presente texto aborda un problema de la suplantación de identidad, haciendo en primera medida una reflexión sobre su rol y amenaza en el marco internacional, en segundo lugar un breve análisis comparado del delito y de los remedios extrapenales existentes en algunos casos, contextualizando el caso colombiano en relación con los de los casos brevemente abordados y enfrentando finalmente la problemática de la inteligencia artificial en un contexto transnacional.

Palabras clave
Derecho penal, derecho al buen nombre y honra, delito de suplantación de identidad, delito informático, bibliometría, ciberseguridad.

Abstract
The present **paper** addresses the issue of identity theft, firstly reflecting on its role and threat in the international framework, secondly providing a brief comparative analysis of the crime and existing extrajudicial remedies in some cases, contextualizing the Colombian case in relation to those briefly addressed, and finally confronting the challenge of artificial intelligence in a transnational context**.**

Keywords
Criminal law, right to a good name and honor, identity theft crime, cybercrime, bibliometrics, cybersecurity.

Introducción

Tanto en el mundo físico como en el ciberespacio la identificación es fundamental para individualizar a la persona, para la prevención del fraude; permite la autenticación verídica garantizando que solo la persona se le respete en todo momento derechos individuales, es de anotar que la acepción “identidad” se relaciona con el reconocimiento personal, los valores que posee, las creencias, su historia, se forma a partir de las experiencias un auto reconocimiento del ser. Dicha acepción es esencial para la participación social es por estas razones y muchas otras que cobra un nivel de importancia su protección y es menester del derecho regular las conductas tendientes a defraudar el uso de la identidad ajena por medio de la suplantación de identidad, un delito que en el escenario de internacional se acoge a las leyes de fraude y abuso de identidad como la Unión Europea con el reglamento general de protección de datos (RGPD) además de la aplicación del derecho interno en cada Estado con leyes que penalizan esta conducta.

La suplantación de identidad es un delito con un nivel de afectación grave a las víctimas, se ramifica de diversas formas, el alcance se materializa tanto en los documentos de identificación físicos como cédulas de ciudadanía o tarjetas DNI como en el ciberespacio, últimamente teniendo una relevancia categórica el universo digital debido a que nos encontramos en un mundo interconectado, se permite la conectividad y comunicación efectiva, la globalización que se ha venido estimulando con el paso a la digitalización, el paso a los entornos digitales ha venido sucediendo durante décadas, solo que se ha venido acrecentando por la información oportuna y responde a los diferentes desafíos como la pandemia COVID 19 que sufrimos como población mundial; el delito de suplantación de identidad merece la atención de los entes gubernamentales, la comunidad académica para los espacios de investigación y mitigación de las diferentes variables que y retos que permitan contrarrestar este delito. La suplantación de identidad es una conducta que se replica a nivel mundial, puesto que en las distintas Constituciones políticas de cada Estado se encuentra la plena identificación de la persona como un derecho fundamental a su individualización, dándole poder a la Ley para desarrollar la regulación pertinente que pudiera hacer frente a las vulnerabilidades y amenazas que subyacen al delito de la falsedad personal, es por las razones de peligro en el fraude que salvaguardar la identidad se ha vuelto primordial categóricamente, en el sentido de que es imperante que en el ámbito penal regule todos los comportamientos tendientes a defraudar.

Se busca proporcionar una comprensión profunda de cómo el Derecho Internacional se adapta y aborda esta creciente amenaza que afecta a la sociedad globalizada en la que vivimos, la suplantación de identidad genera un impacto que trasciende fronteras, afecta directamente a personas, organizaciones e incluso a los distintos entes gubernamentales, desde el fraude financiero, delitos cibernéticos transfronterizos, falsedad en la autenticación y verificación de usuarios en el otorgamiento de crédito de productos financieros, el crimen organizado, espionaje y ciberataques, tráfico de migrantes y documentación falsa, impacto en la reputación en centrales de datos incluso crisis en la seguridad nacional de cada país, entonces es por la anteriores razones que debemos conocer como se ha venido abordando desde el derecho comparado la tipificación de esta conducta, si se requiere ajustes en la normatividad existente en el contexto Colombiano y se es preciso mencionar cómo ha evolucionado y ha tomado nuevas formas la realización de este delito.

¿Hasta qué punto la suplantación de identidad es una amenaza en el ámbito internacional?

La identidad, considerada un derecho humano fundamental, ha sido destacada por autores como Bramont-Arias (2000) como un derecho que el Estado debe garantizar. La violación de estos derechos a menudo implica la participación de fuerzas del orden y operadores legales, y la búsqueda de una solución se facilita cuando hay leyes penales establecidas y un órgano judicial especializado.

En el contexto de la suplantación de identidad, que se ha convertido en una realidad con el desarrollo tecnológico, se argumenta que es necesario establecer una regulación jurídica para garantizar el derecho humano a la identidad. Aunque existen disposiciones legales básicas sobre falsedad personal y documental, como el artículo 296 del Código Penal Colombiano, la legislación actual colombiana a menudo se centra en delitos informáticos de manera general, limitando la especificidad del delito de suplantación de identidad.

Frente a esta problemática, se destaca la necesidad de una regulación global, posiblemente a través de tratados internacionales, que aborden la transnacionalidad del delito de suplantación

de identidad en el entorno digital. Se señala que la legislación local y penal puede ser insuficiente, ya que muchos de los actores involucrados son operadores privados en plataformas digitales. Leyes como SOPA y PIPA, que buscaban proteger los derechos de autor en línea, no abordaron directamente la suplantación de identidad, la ley SOPA (Stop Online Piracy Act) fue desarrollada en EEUU en el año 2011, considerando que frente al avance tecnológico de la digitalización se permita combatir la piratería en línea y las infracciones a derechos de autor en donde el alcance de esta Ley permita tomar acción legal frente a sitios web dedicados a la pirateria, por otro lado la Ley PIPA llega a complementar la actividad limitando las transacciones financieras en estos sitios, dándole poder a los tribunales de distritos EEUU para autorizar el bloqueo de estos sitios.

En tal momento, no se pensó en la suplantación de identidades, con todas las resistencias que estas leyes generaron por tratarse de la protección a formas de propiedad otorgadas a los miembros de la industria de la propiedad intelectual, no se planteó la posibilidad de expandir estos mecanismos de protección a propiedades distribuidas no de industrias, sino de individuos.

En este contexto, se plantea la pregunta de si: ¿se puede responsabilizar a los proveedores de servicios digitales, como redes sociales y microblogs? en casos de alteración de identidad. Se sugiere explorar la posibilidad de medidas cautelares antes los proveedores de los puerto seguros, acciones legales, incluso sin identificar a los perpetradores, para proteger los derechos de los titulares de identidades vulneradas desde el ámbito del derecho privado y las estructuras de propiedad de usuarios e identidades.

En materia de propiedad intelectual, en muchos países, los proveedores de servicios digitales están protegidos por disposiciones legales que los eximen de responsabilidad por el contenido generado por los usuarios. Estas disposiciones, como la Sección 230 de la Ley de Decencia en las Comunicaciones en los Estados Unidos, buscan fomentar la libertad de expresión en línea y la innovación al limitar la responsabilidad de los proveedores de servicios por las acciones de terceros, con base a lo anterior se limita la responsabilidad de los proveedores de servicios digitales, entonces aunque tales proveedores se encuentran amparados legalmente contra la responsabilidad del contenido creado por los usuarios, con base al incremento de este delito, la dinámica legal y regulatoria debe seguir evolucionando y es probable que sigan los debates para determinar responsabilidad de los proveedores de servicios digitales en casos de suplantación de identidad.

En el caso de las identidades, de nombres de usuarios, de avatares, de microblogs, existen unos actores en el marco de la información y protección de datos, en donde la transnacionalidad del delito y su alcance es mayor conforme a la conectividad y crecimiento tecnológico digital se podría definir como una amenaza seria, es de anotar que las lagunas normativas generadas en el uso responsable de las tecnologías de información socava la confianza en las interacciones en línea, toda vez que podría eventualmente afectar la economía digital y la adopción de servicios digitales, la ausencia de seguridad jurídica en el área digital crea desafíos para la persecución legal y la protección de los derechos individuales en el entorno globalizado.

¿De qué manera los ordenamientos jurídicos influyen en la judicialización de Delitos de Suplantación de identidad?

"En la actualidad, la calidad de "sujeto de imputación" que detenta la persona, se extiende a ámbitos que hace algunos años atrás se consideraban inimaginables; como es la tecnología y la red, así como también la posibilidad de que éstos sean medios u objetivos de la comisión de delitos – sean clásicos o informáticos-. Esto se ve directamente relacionado con la existencia de la identidad virtual, la cual se constituye por el conjunto de datos personales con los que las personas interactúan y operan en las redes informáticas, pudiendo ser susceptibles de apropiación no autorizada por su dueño, lo que constituiría delito"(Ferrada Bubniak & Iniescar Medina, 2015), hoy en día en la red se ofrecen variadas y sofisticadas oportunidades de generar delitos de esta índole en cuestión, dando cabida a la ejecución de delitos tanto de naturaleza clásica en el documento físico como de índole informática, lo que expande el universo de posibilidades de ser víctimas, sobre todo en el mundo del Internet, donde las facilidades de comisión están a un "click" de distancia.

Es importante destacar que frente a la evolución en la tecnología que avanza de forma acelerada y continua se formulen sistemas de protección eficientes en donde la "INTELIGENCIA ARTIFICIAL- IA" podría ser una amenaza mayor, si bien hoy en día su incursión puede llegar a crear imágenes, voces sintéticas, videos que pueden ser complejos de diferenciarlos de los reales, podría eventualmente generarse una suplantación de identidad digital, pasamos del formato análogo de documentos físicos alterados a toda una creación digitalizada por medio de IA que cada día toma más fuerza en su implementación en escenarios gubernamentales, académicos, empresariales y sociales, dada su naturaleza de algoritmo de programación avanzado puede acceder a información de datos personales protegidos y hacer su recolección masiva, permitiendo su posible vulneración y puesta en peligro, por ese avance tecnológico que ha venido vivenciando el concepto de "identidad personal" en los distintos escenarios físicos y digitales es donde los ordenamientos jurídicos necesitan ser robustos y específicos en las nuevas modalidades y prácticas en donde se vea inmersa la identidad de la persona y su acceso a datos protegidos legalmente.

En primer lugar el nivel de influencia de los ordenamientos jurídicos va en etapa básica con relación al avance existente del dato personal en el ciberespacio, puesto que en el tipo penal abarca el delito informático en una integralidad de conceptos al acceso y el uso mal intencionado de software para fines delictivos pero no especifica la modalidad de las posibles variantes que pueda obtener la suplantación de identidad, lo que "*se justifica en un enfoque práctico implementar nueva legislación que genere penalidad contundente por la amenaza masiva que refiere el uso de tecnología dando cabida a la necesidad de regulación más estricta porque puede convertirse en un objetivo primordial en política pública estatal ya que se requiere un entorno digital más seguro y protegido para todos".* (Pom, 2023)La influencia del delito de suplantación de identidad puede variar significativamente entre países debido a diferencias en la legislación, regulaciones, tecnologías y cultura. Aquí tienes algunos ejemplos concretos y referencias normativas:

Estados Unidos: En los Estados Unidos, la Ley Federal contenida en el Acta de Fraude y Abuso Informático (CFAA, por sus siglas en inglés) y la Ley de Fraudes y Abusos Informáticos (CFFA, por sus siglas en inglés) son leyes federales que abordan diversas formas de ciberdelitos, incluida la suplantación de identidad en línea.

Impacto en la Privacidad: La suplantación de identidad tiene un impacto significativo en la privacidad individual y puede violar la Ley de Privacidad en Comunicaciones Electrónicas (ECPA, por sus siglas en inglés) en ciertos casos.

Estados Unidos, el delito de suplantación de identidad se encuentra tipificado en el Título 18 del Código de los Estados Unidos, Sección 1028, que establece que:

"(a) Cualquier persona que, con la intención de cometer fraude, fraude electrónico, fraude postal u otro delito, se haga pasar por otra persona o utilice la información de identificación personal de otra persona, será castigada con prisión por no más de 15 años o con una multa de no más de 250.000 dólares, o con ambas."

Unión Europea:
Reglamento General de Protección de Datos (GDPR): En la Unión Europea, el GDPR, representa un avance en normas extrapenales, que establece normas específicas sobre la protección de datos personales. La suplantación de identidad puede violar las disposiciones de este reglamento, y las empresas están obligadas a tomar medidas para proteger la integridad de los datos personales.[1]

España:

En España, el delito se considera contra el patrimonio, mientras que en Estados Unidos se considera contra el orden público. Esta diferencia puede tener implicaciones importantes en la judicialización del delito, ya que los delitos contra el patrimonio suelen ser tratados con mayor severidad que los delitos contra el orden público y reconocen la posibilidad de daño patrimonial y acciones penales o civiles en el marco indemnizatorio.[2]

China:

El delito de suplantación de identidad es un delito grave que puede ser castigado con pena de muerte. Esto se debe a que las autoridades chinas consideran que este tipo de delitos puede tener un impacto negativo en la seguridad nacional. Lo que revela un tamiz del desconocimiento de la identidad como una propiedad del individuo y su contextualización como un bien del Estado[3].

Canadá:

Ley de Protección de la Privacidad en el Sector Privado: Canadá tiene legislación, como la Ley de Protección de la Privacidad en el Sector Privado (PIPEDA), que regula la recopilación, el uso y la divulgación de información personal. La suplantación de identidad podría infringir estas regulaciones.

---

[1] Reglamento General de Protección de Datos (GDPR) en la Unión Europea es un marco legal que establece normas para la protección de datos personales; Articulo 32 Comunicación de una violación de seguridad de datos, artículo 34 (GDPR) comunicación violación de la seguridad de los datos a los interesados.

[2] Artículo 401, que se encuentra en el Título XIII ("De las falsedades") del Libro II del Código Penal España.

[3] Código penal República Popular China, artículo 192 Fraude.

Singapur:

Ley de Delitos Informáticos: Singapur tiene una Ley de Delitos Informáticos que aborda diversas actividades delictivas en línea, incluida la suplantación de identidad. La Ley de Protección de Datos Personales también regula la gestión de la información personal.

Australia:

Ley de Privacidad: En Australia, la Ley de Privacidad de 1988 y las Enmiendas de 2012 establecen principios para la recopilación, el uso y la divulgación de información personal. La suplantación de identidad podría contravenir estas disposiciones.

De otro lado puede concluir que los diversos ordenamientos jurídicos confluyen en la judicialización de los delitos de suplantación de identidad de diversas maneras. En primer lugar, la definición del delito puede variar de un país a otro.

En segundo lugar, el tema probatorio del delito puede variar de un país a otro. En España, la prueba del delito de suplantación de identidad puede consistir en cualquier elemento que demuestre que el acusado se hizo pasar por otra persona. Por ejemplo, la prueba puede consistir en documentos falsificados, testigos presenciales o registros electrónicos. En cambio, en Estados Unidos, la prueba del delito de suplantación de identidad puede ser más compleja, ya que el acusado puede alegar que se hizo pasar por otra persona por error o por razones legítimas, lo que no bastaría con la simple presentación de la evidencia que respalda la acusación, sino que la prueba varía de forma específica con algunos elementos comunes para que pueda ser tomada en cuenta en juicio, procurando que se cumplan los estándares de autenticidad y relevancia en todo el recaudo probatorio.

En tercer lugar, las sanciones por el delito pueden variar de un país a otro. En España, las sanciones por el delito de suplantación de identidad pueden consistir en prisión de tres a seis meses o multa de seis a doce meses. En cambio, en Estados Unidos, las sanciones por el delito de suplantación de identidad pueden consistir en prisión por no más de 15 años o con una multa de no más de 250.000 dólares, o con ambas.

En el caso colombiano no existe directamente un tipo penal centrado en la suplantación de identidades electrónicas, pero si modalidades de delitos que atentan contra la confidencialidad, la integralidad y la disponibilidad de los datos y de los sistemas informáticos que en aspectos tangenciales pueden tener correlación con conductas medio o resultado de la suplantación, como el acceso abusivo a sistema informático (Art- 269A), la obstaculización ilegítima de sistema informático o red de telecomunicación (art. 269B), la interceptación de datos informáticos (art. 269C), el daño informático, el uso de software malicioso o la violación de datos personales, la suplantación de sitios web para capturar datos personales.

Todos los anteriores que recogen de forma fragmentaria y específica conductas que bien sea en la operación de la suplantación o como resultado de ella, pueden producirse.

En conclusión, los ordenamientos jurídicos influyen en la judicialización de los delitos de suplantación de identidad de diversas maneras. La definición del delito, la prueba del delito y las sanciones por el delito pueden variar de un país a otro, lo que puede tener implicaciones importantes en la forma en que se persiguen estos delitos.

Desafío a la estructura legal con suplantación de identidad impulsada por Inteligencia Artificial (IA): La necesidad de regulación normativa

La suplantación de identidad impulsada por la inteligencia artificial (IA) es una creciente amenaza en la era digital con el avance tecnológico, los actores malintencionados pueden utilizar algoritmos de IA para crear perfiles falsos, generar contenido falso y manipular información con un grado de sofisticación sin precedentes. Esto no solo plantea serias preocupaciones en cuanto a la privacidad y la seguridad en línea, sino que también desafía las estructuras legales existentes que rigen el uso de la tecnología. Entonces la IA está siendo utilizada para la suplantación de identidad debido a su lenguaje complejo de programación y es crucial abordar este problema desde una perspectiva legal y ética.

La suplantación de identidad se puede aplicar a varios métodos de comunicación y emplear varios niveles de conocimientos técnicos. Este delito se puede utilizar para realizar ataques de Phishing, que son estafas para obtener información confidencial de personas u organizaciones y que pueden ser utilizadas para emplear *Spoofing*.(Moreno Arvelo & Paucar Paucar, s. f.) modalidades entre muchas otras que los algoritmos pueden evaluar en tiempo real perfiles en redes sociales, uso de ingeniería social precisa y eficaz la falta de regulación es inversamente proporcional al peligro inminente que general el espectro amplio de datos y la accesibilidad que hoy en día cualquier persona tiene en la red.

Es importante tener en cuenta que las implicaciones legales pueden variar significativamente de un país a otro y dependen de la legislación vigente en ese lugar específico, así como de los acuerdos internacionales aplicables. Si se sospecha o se es víctima de suplantación de identidad en un contexto internacional, es esencial buscar asesoramiento legal específico en la jurisdicción que sea relevante.

Profundicemos en el marco ético integral, especialmente en el contexto de la Unión Europea (UE) y el Reglamento General de Protección de Datos (GDPR). Este reglamento es una piedra angular en el enfoque ético de la UE hacia la suplantación de identidad y la inteligencia artificial (IA).

Transparencia:

La transparencia es un principio fundamental del GDPR. En el contexto de la suplantación de identidad, esto implica que las organizaciones deben informar claramente a los individuos sobre cómo se están utilizando sus datos personales y si hay procesos automatizados, como algoritmos de IA, que podrían afectarles.

Consentimiento Informado:

El GDPR enfatiza la importancia del consentimiento informado. Las organizaciones deben obtener el consentimiento explícito de los individuos para procesar sus datos personales. En el

caso de la suplantación de identidad, esto podría implicar la necesidad de un consentimiento específico para el uso de datos en situaciones que podrían involucrar procesos automatizados.

Derecho al Olvido:

Este derecho permite a los individuos solicitar la eliminación de sus datos personales cuando ya no son necesarios para los fines para los que fueron recopilados. En el contexto de la suplantación de identidad, este derecho puede ser crucial para proteger a las personas cuyas identidades han sido comprometidas.

Minimización de Datos:

El GDPR aboga por la minimización de datos, instando a las organizaciones a limitar la cantidad de datos personales que recopilan y procesan. Esto reduce el riesgo asociado con la suplantación de identidad al limitar la cantidad de información disponible para ser mal utilizada.

Seguridad y Protección de Datos:

El GDPR establece la obligación de garantizar la seguridad y la protección de los datos personales. Esto implica implementar medidas técnicas y organizativas para prevenir la suplantación de identidad, como la encriptación y la seguridad robusta en sistemas que manejan información personal.

Evaluación de Impacto de Protección de Datos (EIPD):

Cuando el procesamiento de datos personales, incluida la implementación de tecnologías de IA, podría resultar en un alto riesgo para los derechos y libertades de las personas, se requiere una EIPD. Este proceso implica evaluar y mitigar los riesgos éticos asociados con la tecnología.

Principio de Responsabilidad:

Las organizaciones son responsables de cumplir con los principios del GDPR. Esto significa que deben poder demostrar su conformidad y estar preparadas para asumir la responsabilidad en caso de incidentes, como la suplantación de identidad, que podrían afectar la privacidad de los individuos.

Este marco ético integral busca equilibrar la innovación tecnológica conforme a lo dispuesto (High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence, 2019) con la protección de los derechos individuales. La UE, a través del GDPR, establece un estándar ético sólido que guía el manejo de la información personal en un mundo digital, y estas regulaciones son esenciales para abordar los desafíos éticos asociados con la suplantación de identidad impulsada por la IA.

Por otro lado, los Principios de Asilomar(FLI and developed at the Beneficial AI 2017 conference, 2017), desarrollados por expertos en IA, establecen una serie de directrices éticas y principios para el desarrollo seguro y beneficioso de la inteligencia artificial. Estos principios se centran en aspectos como la investigación a largo plazo, la cooperación internacional y la seguridad. El principio de alineación con los objetivos humanos destaca la importancia de garantizar que la IA actúe de manera coherente con los valores y metas humanas, evitando así la posibilidad de suplantación de identidad con motivaciones perjudiciales.

Enfocarse en los principios éticos de la UE y los Principios de Asilomar no solo proporciona un marco sólido para abordar la suplantación de identidad, sino que también refleja un compromiso con la protección de la privacidad, la equidad y la seguridad en el desarrollo y uso de la inteligencia artificial. Estos principios éticos son esenciales para garantizar que la innovación tecnológica respete los derechos fundamentales y promueva el bienestar social en la era digital. (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, s. f.)

Ahora bien es relevante conocer sobre el principio de centralidad del usuario radica en preservar la dignidad, los derechos y la toma de decisiones autónoma de los individuos en un entorno digital, en la interacción del usuario del comercio electrónico y la implementación de contratos inteligentes (Smart Contracts):

Pérdida de la Centralidad del Usuario:

la preocupación sobre la pérdida de la centralidad del usuario en un entorno donde las máquinas desempeñan un papel cada vez más importante en la toma de decisiones, particularmente en el contexto de contratos inteligentes y el comercio electrónico.(Arenas Correa, 2023), a medida que se automatizan las respuestas y la ejecución de contratos a través de máquinas o algoritmos, hay una pérdida de la centralidad del usuario en el proceso. Esto implica que las decisiones, que antes eran tomadas por los usuarios, ahora están siendo asumidas por máquinas, reduciendo el alcance de la toma de decisiones humanas.

El uso por tanto de las máquinas, sus prestaciones y su programación ética deben respetar la centralidad de los usuarios, propendiéndose por una protección de sus propiedades, identidad y datos en el marco de la prestación de servicios y la potestad decisional de estos usuarios.

Dependencia en Máquinas y Algoritmos:

Se señala la fuerte dependencia de las máquinas, especialmente en la recopilación, selección y comparación de información necesaria para la toma de decisiones. Sin embargo, se destaca la limitación actual de las máquinas para abordar problemas complejos relacionados con emociones, imaginación y sentimientos humanos.

Necesidad de la Decisión Humana Final:

A pesar de la automatización, se argumenta que la decisión final debe permanecer en manos humanas para preservar la autonomía de la humanidad. La sugerencia es que, aunque las máquinas pueden ayudar en la toma de decisiones, la última instancia debe ser una decisión humana.

La centralidad del usuario, esencial para proteger los derechos individuales en entornos digitales, emerge como una defensa clave contra la suplantación de identidad. Al empoderar a los usuarios en la toma de decisiones, se fortalece la prevención de abusos cibernéticos. La suplantación de identidad, un riesgo latente, se ve mitigada cuando los usuarios tienen un rol central en la gestión de sus datos. Este principio no solo fomenta la confianza digital, sino que también resguarda la autonomía y la privacidad. En un mundo donde la tecnología avanza rápidamente, la centralidad del usuario se erige como un baluarte ético y práctico, garantizando que la identidad en línea sea un reflejo fiel del individuo y no un terreno propicio para usurpaciones no autorizadas. En última instancia, al incorporar este principio en el diseño de plataformas y políticas digitales, se crea un entorno más seguro y ético que salvaguarda la integridad de cada usuario en la era digital.

Conclusiones

Con la implementación de leyes y regulaciones, se busca proteger la privacidad y la seguridad de la información personal. Además, es fundamental fomentar la conciencia y educación sobre la ciberseguridad en todos los niveles de la sociedad. Solo a través de una colaboración estrecha entre gobiernos, instituciones académicas y ciudadanos podremos combatir eficazmente la suplantación de identidad y garantizar un entorno digital más seguro y confiable para todos.

En internet las plataformas digitales están muy expuestas al mal manejo de los datos privados, la suplantación identidad como lo vimos anteriormente hacen parte de la orden del día ya que van desde suplantación de documentos físicos hasta los entornos digitales, logrando así que los usuarios no tengan un 100% de seguridad sobre sus datos e información. Los niveles sobre los cuales se puede presentar la suplantación de identidad varían según sea la capacidad y habilidades del hacking implementado, ya que cualquier hacker con conocimientos mínimos de programación y redes puede hacer este tipo de delitos en plataformas con baja seguridad.

Es de vital importancia la implementación articulada de nueva legislación o modificación de la misma que permita hacerle frente al peligro inminente que se encuentra la identidad personal desde el ámbito físico hasta el entorno del ciberespacio, tomando en cuenta que se requiere regulación estricta y especifica frente a cada ramificación o nuevas tendencias en la realización del delito, en los ordenamientos jurídicos del escenario internacional se contempla del delito pero de una forma básica.

Más que una legislación penal fragmentada en multitud de tipos penales específicos sobre diversas conductas tangencialmente relacionadas es necesario establecer medidas desde otros ámbitos del derecho, a que permitan ofrecen protección a través de medidas cautelares y de operaciones transnacionales a los afectados por la suplantación, quienes con mayor rigor gestionarías sus propios derechos.

Por otro lado, la suplantación de identidad, agravada por la inteligencia artificial, destaca la necesidad crítica de regulaciones globales que protejan la privacidad y la autonomía del usuario, enfocándose en la centralidad del individuo como baluarte contra abusos digitales.

La centralidad del usuario, esencial en la era de la inteligencia artificial, no solo fortalece la confianza digital, sino que también se erige como un principio ético crucial para prevenir la usurpación de identidad. Empoderar a los usuarios en la toma de decisiones es fundamental para garantizar la integridad en línea.

Revista modelo: Revista Universidad CES
Link de revisión: https://revistas.ces.edu.co/index.php/derecho/article/view/7169/3838
APA 2023
Referencias: Zotero
ORCID: https://orcid.org/0009-0003-8691-0186

Arenas Correa, J. D. (s. f.). *Remedies to the Irreversibility of Smart Contracts in Colombian Private Law*. file:///C:/Users/Familia/Dropbox/PC/Documents/Downloads/Remedies_to_the_Irreversibility_of_Smart_Contracts%20(1).pdf

Ferrada Bubniak, N., & Iniescar Medina, F. J. (2015). *Usurpación de identidad en las redes sociales Facebook* [UNIVERSIDAD DE CHILE]. https://repositorio.uchile.cl/bitstream/handle/2250/135613/Usurpaci%c3%b3n-de-identidad-en-las-redes-sociales.pdf?sequence=1&isAllowed=y

FLI and developed at the Beneficial AI 2017 conference. (2017). *The Asilomar AI Principles*. https://futureoflife.org/ai-principles/

High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. *2019*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Moreno Arvelo, P., & Paucar Paucar, C. E. (s. f.). Regulación global para evitar la suplantación de identidad digital. *2022/11/01*, 7.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Pom, K. (2023). *A Case Study for Response to Terrorist Crimes Related to Identity Theft in Colorado Springs* [Deparment of Doctoral Studies, Colorado Technical University]. https://www.proquest.com/openview/f793223c0a7596ac738dac93c5fb1245/1?pq-origsite=gscholar&cbl=18750&diss=y