Ciberseguridad: Suplantación de Identidad con el Uso de la Inteligencia Artificial en Colombia, 2022-2025

Yireth Malvaceda Vega[1]

Estefanny Watstein Álzate[2]

Resumen

El presente artículo de revisión analiza el impacto de la inteligencia artificial en la configuración y expansión del delito de suplantación de identidad en Colombia, evidenciando su transformación de una conducta tradicional a una modalidad delictiva mediada por tecnologías avanzadas.

La investigación se desarrolló bajo un enfoque cualitativo, de tipo documental y exploratorio, a partir del análisis de normas, doctrina, jurisprudencia y literatura especializada sobre inteligencia artificial y ciberdelincuencia. Los resultados muestran un rezago normativo frente al acelerado avance tecnológico, así como una limitada efectividad de los mecanismos de prevención y detección, pese a la implementación de soluciones biométricas y herramientas de autenticación digital. Se concluye que, aunque Colombia ha dado pasos importantes como la incorporación de un agravante al delito de falsedad personal, persiste un vacío jurídico que exige el fortalecimiento del marco legal, la creación de políticas públicas especializadas y una mayor educación en ciberseguridad para enfrentar de manera integral la suplantación de identidad mediante inteligencia artificial.

Palabras clave: Inteligencia Artificial (IA), derechos humanos, medidas de protección, protección y legislación colombiana.

[1] Estudiante de derecho Universidad Católica Luis Amigó Yireth.malvacedave@amigo.edu.co

[2] Estudiante de derecho Universidad Católica Luis Amigó Estefany.Wasteinal@amigo.edu.co

Abstract

This review article aims to delve into the impact of artificial intelligence on identity theft in Colombia and how it has transformed the crime from a traditional offense to one that utilizes technology to achieve its objective.

Likewise, this article seeks to broaden readers' understanding of new concepts related to emerging technologies, such as the use of artificial intelligence in crimes like identity theft, which is defined in Article 296 of the Colombian Penal Code as "Personal Falsification."

Furthermore, during the course of this research, it was found that this topic is still being adapted and developed, and that society has very little knowledge about this phenomenon. Therefore, this article serves as compelling evidence of the critical need for a legal framework that can address these new technological advancements.

Keywords: Artificial Intelligence (AI), Human Rights, Protection measures, protection and Colombian legislation.

Introducción

Los avances tecnológicos como lo son las Tecnologías de la Información y las Comunicaciones (TIC), han ido afianzándose a través del tiempo como algo favorable y completamente imprescindible para la vida de las personas actualmente. Así mismo, la criminalidad ha evolucionado de una delincuencia tradicional y se ha convertido en una ciberdelincuencia, por lo tanto, lo que se abordará en este caso son los usos indebidos que se le da a la Inteligencia Artificial (IA) para cometer el delito de falsedad personal.

En relación a Colombia, no se cuenta con una legislación específica en la materia, por lo que es imperativo adoptar un marco jurídico debido a los avances tecnológicos, lo cual implica tomar las medidas pertinentes frente a dicha situación y es por eso que se presentó el proyecto de Ley 225 de 2024, con la finalidad de modificar el artículo 296 del Código Penal Colombiano que corresponde al delito de falsedad personal, adicionando un agravante a la suplantación de identidad de personas que sea realizada a través de Inteligencia Artificial, el cual ha sido aprobado y así mismo, decretada la Ley 2502 el 28 de julio de 2025 para ser aplicada a las

personas que cometen este tipo de delitos en el entorno digital, a partir del año siguiente de su promulgación, es decir, comenzará a regir en el año 2026.

Cabe resaltar que Colombia es pionera en Latinoamérica en la creación de un Marco Ético para la Inteligencia Artificial, el cual fue creado con el objetivo de establecer unos principios que rigen la ética de los datos, de los algoritmos y de las prácticas, la cual es muy importante teniendo en cuenta que se implementará un registro en el que las entidades públicas y privadas, inscribirán sus proyectos permitiendo efectuar un rastreo de los avances que se obtienen de la aplicación de la ética de la Inteligencia Artificial y así fomentar la participación ciudadana responsable.

En consecuencia, los delitos en el ámbito digital se han convertido en un desafío para el derecho por su rápida evolución y constante perfeccionamiento con el paso del tiempo, pues cada vez se hace más difícil detectar la falsedad personal con la ayuda de Inteligencia Artificial pese a que existen algoritmos que son utilizados como mecanismos para ponerlo al descubierto. Cabe resaltar que Colombia se acogió al Convenio de Budapest en virtud de la Ley 1928 de 2018, con el propósito de fortalecer la cooperación internacional y la política penal frente a la ciberdelincuencia.

De este modo, el presente trabajo se orienta a responder el siguiente problema jurídico: ¿qué mecanismos de protección jurídica ha incorporado Colombia, para prevenir la suplantación de identidad con el uso de la inteligencia artificial y cuál es su efectividad?. Frente a este interrogante, el uso indebido de la Inteligencia Artificial plantea importantes desafíos relacionados con la protección de la identidad personal, la dificultad en el ámbito probatorio en los procesos penales y la necesidad de adecuar permanentemente el ordenamiento jurídico frente a las nuevas modalidades delictivas que se cometen por medio de la IA. Si bien el Estado colombiano ha avanzado en la adopción de medidas legislativas y éticas para enfrentar estas conductas, persisten desafíos en la aplicación efectiva de la norma y en el equilibrio entre el desarrollo tecnológico y la protección de los derechos fundamentales.

Metodología

La metodología para abordar esta investigación será cualitativa y está diseñada para trabajarse de forma documental/exploratoria. La técnica de recolección será la revisión bibliográfica de

diversos autores que se enfocan en el estudio de la Inteligencia Artificial y las normas que nacen con el avance tecnológico. Además, se utilizará la técnica analítica-crítica desde un punto de vista subjetivo, en concordancia con los objetivos referidos en esta introducción. Por último, la información se recolectará mediante la búsqueda de normas, doctrina y jurisprudencia de temas concernientes al presente problema, consultando directamente fuentes oficiales del ordenamiento jurídico español.

De manera complementaria, se empleó como herramienta de apoyo la inteligencia artificial ChatGPT (OpenAI) únicamente para la organización preliminar de ideas y orientación en la identificación de normatividad relacionada con el tema objeto de estudio. No obstante, la revisión, selección y verificación de las fuentes utilizadas se realizó directamente en bases de datos académicas y páginas oficiales, garantizando el rigor y la validez de la información incorporada.

Por lo tanto, como autor de referencia para la presente metodología, tendremos en cuenta a Lindsay Prior, quien nos dice que:

> "Los documentos son actores en cadenas de actividad. No son simplemente recursos para la investigación, sino que son elementos constitutivos de la vida social. El análisis de documentos, por lo tanto, no se trata solo de extraer información de ellos, sino de entender su papel en las prácticas y rutinas de la vida cotidiana e institucional" (Prior, 2008, p. 3).

Objetivo General

Describir las diferentes herramientas tecnológicas que son usadas para suplantar la identidad de las personas a través de la inteligencia artificial y los grados de efectividad de los mecanismos de protección y prevención en Colombia, 2022-2025.

Siendo un tema de suma importancia y relevancia, dado que este fenómeno es relativamente nuevo y no tiene una gama amplia de leyes, artículos y jurisprudencia que la respalde. Teniendo en cuenta que esta nueva técnica de suplantación está siendo utilizada por las nuevas generaciones, se tiene claro que se puede dar en todas las ramas del derecho, pero en

específico en el área penal debe ir avanzando a medida que la tecnología lo haga para poder prevenir y sancionar estas conductas que afecten a los individuos en sociedad significativamente.

Objetivos Específicos

Identificar las herramientas tecnológicas y técnicas que son utilizadas para la suplantación de identidad a través de la inteligencia artificial.

Determinar los mecanismos de protección que son utilizados en Colombia para prevenir la suplantación de identidad por medio de inteligencia artificial.

Definir los niveles de efectividad de los mecanismos usados para la prevención de la suplantación de identidad.

Capítulo 1

Tipos de Herramientas Tecnológicas Utilizadas Para la Suplantación de Identidad a través de la Inteligencia Artificial.

El propósito de este capítulo es doble. En primer lugar, se estudiará la evolución tecnológica de los deepfakes, explicando cómo estas técnicas han avanzado y perfeccionado con el tiempo para evadir los sistemas de detección y volverse cada vez más creíbles. En segundo lugar, se abordará de manera fundamental el perfil del ciberdelincuente actual, que ya no es solo un sujeto anónimo y oportunista, sino que presenta una estructura y métodos sofisticados fundamentados en un profundo conocimiento de la psicología humana y los sesgos cognitivos. Esta combinación de tecnología de punta con una estrategia de victimización dirigida ha hecho que el uso del deepfake en actividades delictivas sea especialmente eficaz.

Inicialmente, para suplantar a una persona, lo que el delincuente pretende es obtener la información de estos y para ello se vale de mecanismos, como lo son los malware que es instalado en los dispositivos móviles o computadoras a través de enlaces que envían por correo

electrónico, mensajes de WhatsApp e inclusive mensajes de texto, apropiándose de la identidad de las entidades privadas o públicas con el fin que los individuos se confíen e ingresen sin reparo a estos vínculos, y es ahí en donde se descarga un virus malicioso en los equipos tecnológicos y los datos son extraídos, dejándolos a total disposición de sujetos inescrupulosos.

Cabe resaltar, que los actos cometidos por los delincuentes que utilizan inteligencia artificial y las herramientas empleadas, tienen una fundación teórica conocida como el big five, así lo menciona el autor (Díaz et al, 2023, p. 93):

> El big five de la conducta delictiva, se caracteriza por la energía, entendida como la confianza que denota el delincuente para llevar a cabo la actividad delictiva por su manejo interpersonal de las relaciones que establece con sus víctimas; la afabilidad, que puede ser interpretada por la falta de empatía emocional ante el sufrimiento de sus víctimas o de las personas que llegan a ser parte de sus actividades extorsivas.

En ese sentido, el big five, también conocido como el modelo de los cinco factores o las cinco dimensiones de la personalidad del ciberdelincuente, que es usado en las personas que son elegidas como víctimas para ocasionar un detrimento en su patrimonio. Por lo que los cinco factores se concentran en explicar las cualidades y los rasgos de carácter que son: energía, afabilidad, tesón, estabilidad emocional y por último el modus operandi.

En esta línea, en primer lugar, se tiene la energía, que se entiende como una forma de ingeniería social, la cual despierta en la víctima la confianza suficiente como para que le proporcione información personal al delincuente, dejando en este el manejo total de la situación, pues su habilidad es la manipulación y por ende tiene dominio en las conexiones sociales.

En segundo lugar, está posicionada la afabilidad, el transgresor demuestra ser muy amable, pero la realidad es que no hay sensibilidad alguna por parte de este frente las dificultades que puede atravesar el otro al momento de provocarle un perjuicio.

En tercer lugar, se encuentra el tesón, que es la persistencia que tiene el delincuente al momento de querer lograr su objetivo, pues no tendrá reparo en cómo conseguir la información que necesita, lo que lo lleva a idearse nuevas formas que sean prácticas para engañar fácilmente. En este caso, el avance tecnológico, les ha permitido crear páginas similares a las de los bancos o entidades en donde las personas deban realizar pagos, que sólo al primer vistazo es difícil de

detectar alguna anomalía, lo que conlleva a que ingresen su información personal y claves que son utilizadas para realizar transacciones o desviando los pagos a cuentas que no pertenecen a la entidad que están suplantando como por ejemplo en el caso de EPM, en donde crearon una página idéntica a la real y los pagos que realizaban los usuarios fueron depositados en una cuenta que no pertenecía a la entidad prestadora de servicios públicos.

En la cuarta posición, está la estabilidad emocional, lo que ha dado cuenta de que no son especialmente estables, pues denota intolerancia al fracaso, lo que les genera ansiedad y depresión.

Por último, se encuentra el modus operandi, ya que al ser personas que no tienen emociones y al mismo tiempo no tienen principios, son más conscientes de sus acciones y del desenlace que estas pueden tener. En consecuencia, esto hace que sean más cuidadosos y en la actualidad con la ayuda de la inteligencia artificial, puedan perfeccionar cada vez más sus tácticas de engaño, lo que hace que sea más complicado detectar cuando se está frente a una suplantación.

Ahora bien, como herramienta tecnológica principal están los deepfakes que como concepto tenemos que esta modalidad integra diferentes tipos de contenidos (imágenes, vídeos y audios) que, entrelazados, permiten crear un vídeo falso. Así, los deepfakes pretenden engañar al usuario manipulando un personaje o incluso creando una animación.

Entonces, debe de entenderse que distinguir lo real de lo ficticio en la actualidad es complejo por los grandes avances que tiene la tecnología, por lo que (Mendoza, 2022, p. 62), hace referencia a la forma en la que se percibe lo que se encuentra ante los ojos del ser humano de la siguiente manera:

> Esta tensión es extenuante y nos obliga a tomar posiciones ante lo que estamos viendo en un momento donde realidad y representación ya no tienen por qué guardar ningún nexo (deepfake). Por lo tanto, nuestro viejo aparato crítico ya no tiene elementos de juicio válidos. No podemos establecer un juicio crítico cuando la correspondencia y la coherencia han sido desbordadas (devoradas) completamente por aparatos técnicos (IA).

Dentro de este orden de ideas, se define deepfake como “La generación de contenido audiovisual engañoso o falso mediante la manipulación de imágenes, sonidos o vídeos. Este contenido generado estará descontextualizado en cuanto a tiempo, forma o lugar” (Boté y Vállez, 2022, p. 26).

Es necesario mencionar que el autor (Ayllón, 2024, p. 9) dice:

> Los ‘’deepfakes’’ tienen su origen a finales de 1990, cobraron especial relevancia en el año 2017, a raíz de la publicación de material pornográfico falso a través de la plataforma Reddit 22, donde un usuario anónimo utilizó el rostro de actrices famosas para crear dicho contenido ilícito, conocido ahora como pornografía deepfake no consentida.

De allí, que para (Díaz et al.2023, p. 85) ve el delito tradicional en conjunto con el progreso tecnológico, de la siguiente manera:

> Los delitos tradicionales involucran cada día mayores capacidades tecnológicas y reclutan ciberexpertos que operan con diferentes herramientas, enfoques de ofensa y niveles de anonimato en línea. Esta particularidad del delito informático y de la fusión del delito tradicional con el ciberespacio requiere nuevo conocimiento sobre conductas, factores y características de estos ofensores en línea, con el fin de diseñar estrategias de control y sobre todo de prevención en una sociedad cada vez más conectada.

Los Deepfakes se conforman por unas subdivisiones, como primera subdivisión tenemos los Deepfaces que consisten en crear imágenes convincentes, aunque completamente falsas. Por medio del aprendizaje automático de la inteligencia artificial, se manipulan y generan nuevas imágenes o vídeos a partir de otros y se reemplaza a la persona que aparece en ellos (Dirección de Cómputo y Comunicaciones, s.f.) y como objetivo principal busca manipular datos como imágenes y voz que son usados para fraude, desinformación, acoso.

Como segunda subdivisión tenemos Deepvoice que a diferencia de la anterior esta se basa en la clonación de voz por medio de la inteligencia artificial usada normalmente para realizar suplantaciones de identidad y para afectar la integridad de las personas.

Como tercera subdivisión tenemos Deepfakes de vídeo, a diferencia del anterior Son vídeos falsos creados con técnicas de aprendizaje profundo (deep learning), principalmente mediante redes generativas antagónicas (GANs). Estas redes entrenan algoritmos para imitar rasgos faciales, movimientos y voces, permitiendo suplantar identidades o alterar acciones en grabaciones reales (SEON, s.f).

En relación a las Redes Generativas Adversariales (GAN), (Franganillo, 2023, p.5) las define como:

> Para ello, emplean redes generativas adversariales, esto es, sistemas de IA que se entrenan mediante el aprendizaje profundo (deep learning) a partir de grandes cantidades de datos. Este logro tecnológico tiene un lado amable y hasta lúdico, dado que permite producir con suma facilidad imágenes de un realismo sorprendente, pero también esconde problemas y riesgos que requieren atención.

De allí, que para detectar un deepface, lo que se busca son los rasgos ajenos de lo vivo, que se muestran como incoherencias que presentan las imágenes, como lo es el movimiento facial natural, el parpadeo y la luz.

Igualmente, los deepfakes se han convertido en una amenaza, porque se están utilizando de forma maliciosa para engañar a otros con fines de lucro, suplantando la identidad de otra persona, utilizando su rostro, su voz y su información. Hay que destacar que no es algo nuevo, pues viene de mucho tiempo atrás ya que era una técnica que se realizaba a mano, en donde se hacían retoques y actualmente es algo que se le delega en su totalidad a los ordenadores por medio de softwares que lo hacen de forma automática, dando como resultado un contenido muy realista que es difícil de detectar como falso

Conforme a ello, tenemos que en 2017 unos investigadores de la Universidad de Washington utilizaron más de 14 horas de grabación del presidente Barack Obama para reproducir su imagen y voz, y así simular cualquier discurso. Crearon un modelo de la forma y los movimientos de la boca para vincularlo con las grabaciones de la voz. Con esta técnica, partiendo de vídeos reales podrían poner en boca de Barack Obama cualquier mensaje que un actor reprodujera.

Por otra parte, en 2018 un grupo de profesionales hizo un Deepfake, del senador de Texas Ted Cruz cantando e imitando a Tina Turner. En este caso, el modelo de algoritmos codificó cómo gesticula, se mueve y se ve la cara del senador y la de un actor. A continuación, decodifica las imágenes del rostro de Ted Cruz y las reconstruye sobre las del rostro del actor (Visus, 2021, párr. 6).

Según esta referencia se puede evidenciar los alcances que esto ha tenido en la sociedad a lo largo de los años, además, no sólo se falsifica la parte física de una persona como lo es el rostro, ahora esto ha llegado mucho más lejos y es la suplantación de la voz que tampoco es algo nuevo. Todo inicia con los convertidores de voz, lectores de pantalla y en la actualidad se tiene los sistemas generadores de voz a través de la inteligencia artificial que permiten que, por medio de una videoconferencia, con la imagen y la voz, hace que sea mucho más fácil engañar, lo que lo hace un reto cada vez más grande para la ciberseguridad.

Los fenómenos de criminalidad que afectan la Ciberseguridad son generados, en muchas ocasiones, por actores que se encuentran en una jurisdicción geográfica diferente en la que se comenten los delitos, por lo que las pruebas de un acto delictivo no son accesibles sin la colaboración judicial y técnica de las legítimas autoridades públicas que rigen sobre ese territorio. Por lo tanto, en este marco y en los casos que suponen la utilización de redes de comunicación, la cooperación internacional es esencial para prevenir y enfrentar cualquier acto delictivo en materia cibernética, por ello Colombia se adhirió al Convenio sobre la ciberdelincuencia del Consejo de Europa del 2018.

Por consiguiente, la ciberseguridad puede verse afectada por una de las modalidades de suplantación de sitios web como lo es el phishing, que es usada por los ciberdelincuentes con la finalidad de extraer la información confidencial de las personas que están siendo previamente engañadas al recibir correos electrónicos con enlaces de páginas falsas o mensajes de texto que es una variante del phishing llamada smishing, además, existe el spoofing que es utilizado para crear ambientes falsos para obtener claves, realizando el cambio IP o de servidores (Martínez, 2024, p.10).

Phishing

Phishing es la combinación de Ingeniería Social y exploits técnicos, diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante. La mayoría de los ataques de Phishing son influenciados cuando se envía un correo electrónico falso, que contiene un enlace (Uniform Resource Locator, URL). Esta URL conduce a un sitio web falso, cuando se hace clic en él. A pesar de la importante atención que se le ha otorgado a lo largo de los años, aún no existe una solución definitiva, para resolver este tipo de ataque (Benavides et al, 2020, p. 98).

Así mismo en Latinoamérica, el phishing es uno de los delitos más usuales para suplantar la identidad de las personas con el propósito de conseguir información sensible y es visto más comúnmente en el ámbito financiero, por lo que las entidades bancarias han tenido que implementar tokens con el fin de que las transacciones tengan un rango de seguridad más alto, para evitar que los datos de las personas sean robados y usados para sustituir la personalidad de alguien más.

También, puede estar en una plataforma de mensajería como lo es el WhatsApp, en donde llegan mensajes con un enlace en donde la persona que ingresa a este lo que hace sin saberlo es aprobar la suplantación de identidad, pues es un método en donde aparentemente la persona dueña de la información está realizando una transacción.

Así pues, una de las variantes del phishing es el smishing el cual está basado en correos, mensajes de texto y llamadas realizadas por los ciberdelincuentes para engañar a los usuarios financieros y obtener información valiosa, como los datos de usuario y clave de acceso a las plataformas virtuales, haciéndose pasar por agentes de la entidad bancaria. Con esta modalidad de estafa los ciberdelincuentes se apropian de todos los datos necesarios para poder realizar movimientos bancarios a nombre de las víctimas (Cañas Quiroga, Cuéllar Sosa, & Marín Aguirre, 2021, p. 18).

Smishing

La diferencia entre las modalidades de phishing son los medios por los cuales se lleva a cabo, en este caso, el smishing es más propenso a ser efectivo porque en los equipos móviles no se maneja un filtro, como en el caso del correo electrónico en donde hay una bandeja llamada

spam que advierte al usuario de que puede ser algo malicioso con lo que debe tenerse cuidado al darle clic.

Por lo tanto, el "Smishing es un ataque de ingeniería social que emplea mensajes de texto falsos para persuadir a individuos a que instalen malware, compartan datos personales o transfieran dinero a criminales informáticos". ("¿Qué es el smishing (phishing por SMS)?", 2024, párr. 1)

Es conveniente resaltar que, el mensaje de texto puede llegar a ser más persuasivo, pues es mucho más fácil que alguien pueda confundirse o simplemente que en un descuido entre al enlace que se le está enviando para verificar de qué se trata, y es ahí en donde el delincuente informático se aprovecha obteniendo información al instalar en el dispositivo móvil un virus, lo que se convierte en una amenaza constante para la seguridad de todas las personas.

Por ejemplo, un SMS que contiene un enlace falso de una entidad bancaria, en donde solicitan el cambio de clave, actualización de información o en algunos casos se trata de un préstamo o tarjeta de crédito que el supuesto banco le aprobó y que puede obtener este beneficio con sólo ingresar y seguir los pasos que se envía en el mensaje.

Spoofing

Es un método que es utilizado para inducir al error a las personas, disfrazando o imitando las personas jurídicas como bancos o en algunos casos empresas que venden productos o servicios. En consecuencia, lo que se pretende es que las personas ingresen sus datos personales para apoderarse de ellos y así llevar a cabo la suplantación de identidad de los usuarios ante estas entidades.

Por esta razón es muy importante verificar qué fallo pueden presentar las páginas web, que aunque son muy similares a simple vista, pueden tener algunas características diferentes que permitan determinar que es un engaño.

Como indica el autor (Martínez, 2024, pp. 6-7):

> Es el denominado spoofing desde un punto de vista criminológico, consistente en una técnica habitualmente utilizada por los cibercriminales, que supone la suplantación

de la identidad de una persona física o jurídica con distintas finalidades y para la realización de infracciones de muy diverso tipo.

En efecto, las infracciones que pretenden cometerse por estos sujetos generalmente son de índole económico, pues así han logrado desviar pagos de otras entidades, comprar productos o servicios a nombre de la persona suplantada y en otros casos sacar el dinero de las cuentas bancarias de sus víctimas. Además, existen otros tipos de spoofing como lo son:

Email spoofing: en este caso se trata de suplantar una dirección de correo electrónico de una persona o compañía. Normalmente, suelen suplantar la de compañías con gran notoriedad. Y es que, al igual que en el resto de ataques, se busca la confianza de sus posibles víctimas para que caigan en la trampa. De esta forma, quieren conseguir información confidencial o hasta infectar los dispositivos de los usuarios al hacer que se descarguen apps maliciosas. Además de que también se suele usar para mandar correos Spam y hasta cadenas de bulos.

DNS spoofing: se consigue mediante la ejecución de softwares que son maliciosos o, por otra parte, aprovechan las vulnerabilidades en las medidas de protección con tal de lograr modificar los DNS. La finalidad de este tipo de ciberataque es conseguir que los usuarios terminen accediendo a una web específica que ha sido manipulada y creada por los piratas informáticos para el robo de datos.

IP spoofing: esta variante en particular consiste en la falsificación y sustitución de la IP por otra que es falsa. Los ciberdelincuentes consiguen acceder a diferentes redes en las que las víctimas se autentican o, incluso, en aquellas en las que se conceden diferentes permisos (Redeszone, 2024, párr. 8).

En síntesis, es necesario que las personas tanto naturales como jurídicas tomen medidas de autocuidado, para evitar ser víctimas de este tipo de delitos, deteniéndose al momento de recibir un correo electrónico o un mensaje de texto, leer de forma meticulosa ya que en con un solo clic pueden entregar toda su información y los ciberdelincuentes pueden obtener los datos personal y sensibles, ocasionando daños económicos y morales de los que luego no pueden recuperarse. Deben tenerse en cuenta los productos y servicios que las personas tienen contratados, pues si llega una notificación de algo que no se ha comprado o contratado, es un

indicio para desconfiar e intuir que puede tratarse de un engaño y las personas jurídicas deben reforzar sus sistemas de seguridad y controles.

Capítulo 2

Mecanismos De Protección Que Son Utilizados En Colombia Para Prevenir La Suplantación De Identidad Por Medio De Inteligencia Artificial.

El objetivo central de este análisis es realizar un examen integral del marco de defensa existente. Para ello, se estructurará la investigación en tres pilares fundamentales: primero, se revisará el marco normativo y jurídico, explorando la eficacia de leyes como el Código Penal Colombiano (Ley 599 de 2000) en tipificar la suplantación de identidad, y la capacidad de las autoridades, como la Policía Nacional y la Fiscalía General de la Nación, para investigar estos delitos. Segundo, se evaluarán las herramientas y soluciones tecnológicas disponibles, tanto a nivel estatal como privado, para la detección y verificación de contenidos falsos. Finalmente, se considerarán las estrategias de concientización y educación digital promovidas por el gobierno y otras entidades, dirigidas a formar una ciudadanía más crítica y resiliente frente a la desinformación y el fraude digital.

Es necesario decir que en Colombia se tipificó el delito de falsedad personal a través de la Ley 599 de 2000, pues en aquel tiempo no había un desarrollo tecnológico como el que se tiene el día de hoy, pues la suplantación se hacía utilizando documentos adulterados como la cédula de ciudadanía, lo que conllevaba a que se infringiera en una variedad de delitos como lo es el de falsedad material en documento público, el cual se encuentra estipulado en el artículo 287 del Código Penal colombiano, pues se altera la parte física del documento, todo con la finalidad de hacerse pasar por otra persona y obtener beneficios económicos o legales.

Además, en ocasiones no era necesario modificar el documento público, pues en caso de que la persona presentara características físicas similares a la persona propietaria del documento, al no existir un método de verificación de identidad como la biometría o pruebas de identidad que se realizan con la finalidad de determinar, que sí es la persona real, era muy fácil que el delincuente obtuviera el servicio o producto a nombre de otra persona.

Como se anotó anteriormente, referente a las características físicas el autor (Medina, 2013, p. 2), indica qué son:

> Las características de atributos fisiológicos son consistentes, puesto que no cambian en el tiempo, salvo que sean alteradas por alguna enfermedad, trabajo o accidente el cual varía la morfología de estas propiedades en las personas, mientras que el comportamiento tiene un margen de menos consistencia, porque dependen directamente de la naturaleza o personalidad humanas.

Por otra parte, no quiere decir que en la actualidad no sea posible que la suplantación de identidad para el delincuente no sea exitosa, ya que haciendo uso de un documento público que no le pertenece, pudo obtener de forma previa la información personal de la persona que quiere afectar, lo que quiere decir que si se le hace por parte de una entidad una prueba de identidad, es posible que la apruebe sin problema alguno.

Es decir, en estos casos conseguir la información personal no es un problema mayor para quien delinque, puesto que, muchas de las aplicaciones que se descargan en los móviles, o por medio de páginas web o con una llamada, pueden obtener información para suplantar a una persona sin dificultad. Por ello es de vital importancia que en Colombia pueda regularse este tipo de delitos.

En segundo lugar, como medio de protección de los derechos y deberes de las personas se encuentra la Constitución Política de Colombia de 1991, en su artículo 15 se describe del derecho a la intimidad que reza:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
>
> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

No obstante, el delincuente actual vulnera este derecho tan importante en todo sentido, al hurtar la información acudiendo a diferentes modalidades, ocasionando un daño patrimonial y al buen nombre de quién es víctima de este cometido.

De la misma forma, se ve afectado el derecho a la honra, consagrado en el artículo 21 de la Constitución Política de Colombia de 1991, en tanto la suplantación de identidad involucra de forma directa la reputación y el buen nombre de las personas, ocasionando consecuencias negativas en su esfera económica y financiera. De conformidad con ello, la Ley 1273 de 2009 refuerza la protección penal frente a la utilización indebida de datos personales y mecanismos de identificación, reconociendo la especial gravedad de estas conductas por su impacto en la confianza y seguridad de las relaciones jurídicas. En este sentido, se trata de un delito de carácter pluriofensivo, pues no solo vulnera la honra y el buen nombre, sino que también afecta bienes jurídicos como el patrimonio privado y la fe pública.

Por otra parte, es de gran importancia que los derechos fundamentales que deben garantizar el derecho información y a la privacidad de los ciudadanos sean respaldados, por eso, cabe mencionar la Ley 527 de 1999 que tiene como fin brindar seguridad jurídica a la información que sea de dimensión electrónica, cumpliendo la misma función de la firma tradicional, que es la física. En su artículo 2, literal c, define la firma digital como:

> Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

De este modo, le da fuerza obligatoria a los documentos que sean firmados por este medio, ya sea en contratos o mensajes de datos.

Es importante decir que, en el Decreto 2364 de 2012 en su artículo 1°, numeral 3, se define como Firma electrónica:

> Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Fundamentalmente, uno de los principales objetivos de esta ley es buscar que se cumpla y que sea confiable para las personas el uso de las nuevas tecnologías y así mismo que la protección de sus datos esté resguardada de una manera segura, además de esto los efectos que tiene la firma electrónica serán los mismos de la firma habitual siempre que cumpla con las características estipuladas.

Siguiendo con lo anterior, hay otro método de protección de datos que se llama la huella digital derivada de la huella dactilar, este ha sido siempre el rasgo biométrico utilizado por la humanidad, desde el siglo pasado, para la identificación de las personas. Es un rasgo particular de cada individuo, cuya formación tiene lugar durante la etapa fetal y permanece inmutable a lo largo de toda la vida. La huella dactilar permite, además, discriminar perfectamente a los individuos. (Rojas & Suárez, 2018, p.39).

En adelante, cabe mencionar que Colombia es un país en el que se ha vuelto común la ciberdelincuencia, por lo cual se ha visto en la necesidad de implementar una modificación al artículo 296 del Código Penal colombiano que regule el uso indebido de la IA, por ello, se mencionarán los proyectos de ley que se han ido proponiendo en los últimos años y estos son:

Proyecto de Ley N 354/2021 Cámara.

A través de este se establecen los lineamientos de política pública para el desarrollo, uso e implementación de Inteligencia Artificial y se dictan otras disposiciones. (Echavarría et al. 2021).

Proyecto de Ley N 253/2022

Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de inteligencia artificial y se dictan otras disposiciones. Senado de la República de Colombia. (2022).

Proyecto de Ley 200/2023

Así pues, se define y se regula la inteligencia artificial, se establecen límites frente a su desarrollo, uso e implementación y se dictan otras disposiciones. (Cortés et.l. 2023).

Proyecto de Ley 225/2024

El objeto de este es modificar el artículo 296 de la Ley 599 de 2000 Código Penal Colombiano, con lo cual se trata de adicionar un agravante (una circunstancia que aumenta la pena) del delito de falsedad personal (usar identificaciones falsas o ajenas), cuando este se realice por medio de IA. Es una iniciativa que fue aprobada en el año 2025, convirtiéndose así en la Ley 2502 de 2025 que entrará en vigencia a partir del año 2026.

Además, se encuentra en curso el Proyecto de Ley 043 de 2025 radicado ante el Senado de la República el 28 de julio de 2025 por el señor Diego Alejandro González, en virtud de regular la Inteligencia Artificial en Colombia con la finalidad de que su uso se haga de forma responsable y ética.

Es conveniente decir, teniendo en cuenta los anteriores proyectos de ley citados, se puede observar que en Colombia en muchas ocasiones se ha intentado llevar a cabo una ley que busque proteger los derechos de las personas tanto jurídicas como naturales entorno al uso indebido de la tecnología, por lo que en el año 2025 aunque no se logró crear un tipo penal independiente se creó un agravante para el delito de falsedad personal.

De igual forma, es conveniente garantizar los principios constitucionales, por lo que se han desarrollado leyes que ayuden a la su protección y a mitigar este fenómeno. En Colombia unos de los instrumentos que se han venido implementando es la Ley 1266 de 2008 la cual

regula el hábeas data y el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Así mismo, otra ley que hace una parte súper importante del tratamiento de datos es:

La Ley Estatutaria 1581 de 2012. Artículo 1: Objeto.

> La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

También, en el artículo 6° de la *Ley 1581 de 2012*, se menciona:

> Tratamiento de datos sensibles se prohíbe el tratamiento de datos sensibles —que son aquellos que pueden afectar la intimidad del titular o cuya utilización indebida puede generar discriminación (origen racial o étnico, orientación política, convicciones religiosas o filosóficas, salud, vida sexual, datos biométricos, etc.).Congreso de Colombia. (2012).

Puesto que, tiene como fin que sea aplicada a los datos personales registrados en cualquier base de datos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. Esto incluye información como nombres, documentos de identidad, direcciones, estados civiles, entre otros, brindando una protección integral.

Se puede señalar, que la Ley 1712 del 2014, en su artículo 1°, se conoce como la ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, teniendo como objetivo principal el siguiente artículo. "El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.''

En esta ley hacen parte 10 principios los cuales son:

1. Principio de transparencia:

Está sujeto al deber de proporcionar y facilitar el acceso a la información en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley.

2. Principio de Buena Fe:

En virtud del cual todo sujeto obligado, al cumplir con las obligaciones derivadas del derecho de acceso a la información pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.

3. Principio de Facilitación:

En virtud de este principio los sujetos obligados deberán facilitar el ejercicio del derecho de acceso a la información pública, excluyendo exigencias o requisitos que puedan obstruir o impedirlo.

4. Principio de no Discriminación:

De acuerdo con el cual los sujetos obligados deberán entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivación para la solicitud.

5. Principio de gratuidad:

Según este principio el acceso a la información pública es gratuito y no se podrá cobrar valores adicionales al costo de reproducción de la información.

6. Principio de celeridad:

Con este principio se busca la agilidad en el trámite y la gestión administrativa. Comporta la indispensable agilidad en el cumplimiento de las tareas a cargo de entidades y servidores públicos.

7. Principio de eficacia:

El principio impone el logro de resultados mínimos en relación con las responsabilidades confiadas a los organismos estatales, con miras a la efectividad de los derechos colectivos e individuales.

8. Principio de la calidad de la información:

Toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable

9. Principio de la divulgación proactiva de la información:

El derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad.

10. Principio de responsabilidad en el uso de la información:

En virtud de este, cualquier persona que haga uso de la información que proporcionen los sujetos obligados, lo hará atendiendo a la misma. Congreso de Colombia. Congreso de Colombia. (2014, marzo 6). Ley 1712 de 2014, Principios que tienen como principal objetivo, facilitar la protección de datos personales.

Por otra parte, tenemos el convenio de Budapest que es el primer tratado internacional que busca abordar los delitos informáticos del internet a nivel internacional facilitando así mismo la persecución de estos en el ámbito transnacional. “En esa medida, se prevé la creación de una red que opere 24 horas de los 7 días de la semana, para garantizar una rápida cooperación internacional que reaccione frente a algún tipo de incidente” (Mintic, 2025, párr. 4).

Este convenio desarrolla varios conceptos que son de suma importancia para la realización de este trabajo. Según los efectos del Convenio de Budapest (Consejo de Europa, 2023, pp. 8-9):

A) Sistema Informático: designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos.

b) Datos Informáticos: Designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función.

c) Prestador de Servicios: Designa a toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático.

Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios.

En otro orden de ideas, se puede decir que Colombia se vinculó al Convenio de Budapest el 16 de marzo de 2020, adhiriéndose así mismo a las políticas y las medidas legislativas tanto para personas naturales como jurídicas planteadas en el mismo, este tratado marcó un paso importante en la historia de la tecnología en Colombia dando paso a compartir medidas en cuanto al artículo 25, Principios generales relativos a la colaboración "Los Estados firmantes acordarán llevar a cabo una colaboración lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal"

Por otro lado, la Ley 2502 de 2025 que modifica el artículo 296 del Código Penal Colombiano (Ley 599 de 2000) para incluir un agravante específico cuando el delito de falsedad personal se comete utilizando Inteligencia Artificial (IA), especialmente en casos de suplantación de identidad mediante técnicas como *deep fakes*. Además, establece lineamientos para la formulación de políticas públicas destinadas a prevenir y controlar el uso indebido de la IA en la cual se ordena la creación de una política pública que incluya:

- Marco ético para el uso de IA.
- Colaboración intersectorial.
- Educación y capacitación en ciberseguridad y ética digital.
- Desarrollo tecnológico y herramientas de detección de deepfakes.
- Transparencia y gobernanza de IA.
- Cooperación internacional.
- Protocolos de respuesta rápida.

No obstante, podemos identificar que esta herramienta tiene como función principal reforzar las aplicaciones que facilitan el acceso a los datos.

Dentro de esta línea, en Colombia a lo largo de los años se han venido emitiendo varias sentencias que tienen un enfoque sobre el tema que se está tratando en este artículo, como primera sentencia tenemos la sentencia SP 592-2022 que tiene como hechos principales:

“1. En 2013, la Fiscalía imputó a varios involucrados, incluyendo a Cubides Muñoz y Malaver Molina, por delitos como concierto para delinquir, falsedad en documento privado, estafa continuada y acceso abusivo a sistema informático agravado”.

Por una parte, en el año 2016 se emitió un fallo condenatorio para algunos acusados. Posteriormente, en apelación en 2017, se confirmaron las condenas por concierto para delinquir y acceso abusivo a sistema informático agravado para Cubides Muñoz y Malaver Molina. En donde se determinó que las acciones delictivas de los condenados, se configuraron al acceder a datos personales sin la autorización de las personas, generando así mismo fraudes que afectaron la seguridad y patrimonio de Davivienda, las pruebas que fueron utilizadas para emitir la sentencia fueron testimonios de funcionarios del banco y análisis detallados de las irregularidades en las consultas realizadas por los acusados.

Según la sentencia SP 592-2022 de Corredor, se puede ver claramente los delitos cometidos por los infractores y las consecuencias que acarrea este como lo es la mala protección de datos y la falta de implementación de mecanismos que protejan tanto a la persona jurídica como a las personas naturales.

Así mismo, tenemos la sentencia 053606099057 2021-50679 en donde se trata el “HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. parámetro adicionado por el artículo 1 de la Ley 1273 de 2009, Tribunal Superior de Medellín, Sala de Decisión Penal 2022. Proceso No. 053606099057 2021-50679. en donde se puede establecer la vulneración de datos de manera abusiva por parte de los infractores, mediante el uso de medios informáticos.

Además, en este ámbito de suplantación de identidad podemos encontrar que de manera infructuosa se han presentado acciones de tutelas en contra de personas jurídicas, como la acción de tutela presentada por Ismael Silva Rodríguez en contra del Banco Davivienda S.A. Corte Constitucional de Colombia, Sala Sexta de Revisión (2022). Sentencia T-8.727.419. Magistrado ponente: Hernán Correa Cardozo, en donde la accionante alega que se le fueron vulnerados lo derechos fundamentales como el buen nombre, el debido proceso y habeas data, en donde el Juzgado Promiscuo Municipal de Sabana de Torres lo declaro improcedente, porque, no es el medio determinado para la protección de esos derechos.

En Colombia es evidente el gran atraso normativo en cuanto a la regulación de las nuevas tecnologías de la comunicación y de la información y la IA, y es hasta el año 2025 que surge un agravante para el delito de falsedad personal, en cuyos casos la suplantación se realice por medio de la IA, pero no lo tipifica, como tipo penal independiente.

Análisis comparativo entre Colombia y España.

A continuación, se realizará un análisis comparativo entre el avance normativo de España y Colombia en materia de regulación del uso de las tecnologías digitales. Conviene destacar que se abordarán conceptos como los deepfakes, la suplantación personal, la identidad y el derecho a la propia imagen.

La Fiscalía General del Estado ha advertido que los riesgos asociados al uso de tecnologías digitales exigen una adaptación constante en materia de seguridad de la información, especialmente frente a conductas como la suplantación de identidad y otros delitos tecnológicos (Fiscalía General del Estado, 2023, p. 87).

En este sentido, resulta de gran importancia subrayar que España ha mostrado un mayor desarrollo normativo, al haber impulsado proyectos de ley que ya han sido incorporados en su legislación. Dichas iniciativas tienen como principales objetivos la prohibición y sanción de conductas que atenten contra la identidad personal, la imagen y la dignidad de las personas, especialmente cuando estas son afectadas mediante el uso de tecnologías de manipulación digital, por lo tanto, sus principales focos es prohibir:

1. El uso de técnicas subliminales (imágenes o sonidos imperceptibles) para manipular decisiones sin consentimiento, causando un perjuicio considerable a la persona (adicciones, violencia de género o menoscabo de su autonomía)

2. Explotar vulnerabilidades relacionadas con la edad, la discapacidad o situación socioeconómica para alterar sustancialmente comportamientos de modo que les provoque o pueda provocar perjuicios considerables (Ejemplo: Un juguete infantil habilitado con IA que anima a los niños a completar retos que les producen o pueden producirles daños físicos graves)

3. La clasificación biométrica de las personas por raza u orientación política, religiosa o sexual.

4. La puntuación de individuos o grupos basándose en comportamientos sociales o rasgos personales como método de selección para, por ejemplo, denegarles la concesión de subvenciones o préstamos.

5. Valorar el riesgo de que una persona cometa un delito basándose en datos personales como su historial familiar, nivel educativo o lugar de residencia, con excepciones legales.

6. Inferir emociones en centros de trabajo o educativos como método de evaluación para promoción o despido laboral, salvo por razones médicas o de seguridad. España (Ministerio para la Transformación Digital y de la Función Pública, 2025, p. 2).

Por otro lado España tiene una normativa que surge desde la : Estrategia Nacional de Inteligencia Artificial (ENIA) - Actualizada 2023, que tiene como aspecto relevante que La AEPD y la Comisión Europea han emitido dictámenes (2023-2024) sobre el uso de IA, enfatizando que el reconocimiento facial en espacios públicos es de "alto riesgo" y generalmente prohibido bajo el RGPD, siendo este un país en donde han habido casos como este en donde se interpuso una multa de €100,000 a una empresa por usar sistemas de vigilancia con reconocimiento facial sin base legal. según la Agencia Española de Protección de Datos. (2023). *Resolución del Procedimiento PS/00400/2022 (Fuente Académica Deep Seek p 10-13).

Dentro de este marco, el *Código Penal español* (Ley Orgánica 10/1995, de 23 de noviembre) tipifica en su artículo 401 el delito denominado usurpación del estado civil, estableciendo que: “El que usurpare el estado civil de otra persona será castigado con la pena de prisión de seis meses a tres años” (art. 401).

También es Estado miembro al igual que 26 Estados más del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por medio de este se establecen normas para regular la Inteligencia Artificial, siendo un mecanismo de prevención pues limitan a los diferentes sistemas de IA como lo son Gemini, ChatGPT y otros, para que cumplan con ciertos

requisitos como lo es clasificar el contenido creado por esta y evitar producir material ilegal como lo es el caso de la pornografía infantil.

Es importante decir, el impacto que tiene la Unión Europea en cuanto a la regulación de la Inteligencia Artificial es significativa en comparación con Colombia, pues en España ya se tiene una Institución llamada AESIA (Agencia Española de Supervisión de Inteligencia Artificial) la cual tiene el objetivo:

> La Agencia Española de Supervisión de Inteligencia Artificial es el organismo público encargado de garantizar el uso ético y seguro de la inteligencia artificial en España. Su principal misión es asegurar que tanto entidades públicas como privadas cumplan con la normativa vigente, protegiendo la privacidad, igualdad de trato y derechos fundamentales.
>
> La AESIA fomenta un desarrollo tecnológico responsable, trabajando en colaboración con otros organismos y promoviendo un entorno de confianza para el avance de la inteligencia artificial, asegurando que sea beneficioso y seguro para la sociedad. (AESIA, párr. 1-2).

Contrario a lo que se presenta en España, en Colombia aún no existe una autoridad para que promueva y fomente el desarrollo y uso responsable de la Inteligencia Artificial, lo cual demuestra un atraso considerable frente a España.

En definitiva, resulta evidente que Colombia aún tiene un amplio camino por recorrer en materia de regulación penal de las conductas delictivas cometidas mediante el uso de la Inteligencia Artificial. Si bien han existido antecedentes normativos, como diversos Proyectos de Ley orientados a actualizar el ordenamiento jurídico frente a estas nuevas formas de criminalidad, lo cierto es que no se ha logrado la creación de un tipo penal autónomo que incorpore expresamente estas conductas dentro del Código Penal colombiano. En consecuencia, el único avance normativo significativo se materializó hasta el año 2025, cuando se optó por introducir un agravante al delito de falsedad personal, previsto en el artículo 296 de la Ley 599 de 2000, para los casos en que la conducta sea cometida mediante el uso de Inteligencia Artificial.

En contraste, el ordenamiento jurídico español evidencia un desarrollo normativo más sólido y sistemático en esta materia. A través de la Ley Orgánica 10/2022, en el artículo 172 ter. numeral 5 dice:

> El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillante, será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses. Si la víctima del delito es un menor o una persona con discapacidad, se aplicará la mitad superior de la condena.

En efecto, España incorporó expresamente la suplantación de personalidad en el entorno digital como una modalidad relevante para la usurpación del estado civil, reforzando la protección penal frente a conductas realizadas a través de internet y tecnologías emergentes. En este sentido, el Código Penal español regula el delito de usurpación del estado civil dentro del Título XVIII, castigando a quien asuma la identidad de otro con trascendencia jurídica, siendo esta regulación extensible a los supuestos en los que dicha suplantación se lleve a cabo por medios digitales, redes sociales o herramientas tecnológicas, en coherencia con la realidad actual de los delitos informáticos.

Adicionalmente, España se erige como un modelo a seguir al haber creado instituciones especializadas como la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA**)**, encargada de regular, supervisar y coordinar los asuntos relacionados con el uso de la Inteligencia Artificial, incluida su eventual utilización para la comisión de delitos, lo que demuestra un enfoque integral y preventivo frente a los riesgos que estas tecnologías representan para los derechos fundamentales.

Por último, se torna relevante que Colombia dé un cambio de enfoque en cuanto a sus leyes, pues es necesario que estas se actualicen de forma considerable, en la medida en que el delincuente común ha mutado a ciberdelincuente. Si bien el Estado colombiano dio un primer avance con la expedición de la Ley 1273 de 2009, mediante la cual se incorporaron al Código Penal nuevos tipos penales orientados a la protección de la información y de los datos, dicha normativa resulta insuficiente frente a la evolución de la tecnología y de las modalidades

delictivas. En efecto, no todo criminal delinque en las calles, sino que muchos lo hacen a través de una computadora, haciendo uso de herramientas tecnológicas cada vez más sofisticadas, lo que les permite burlar con mayor facilidad la autoridad. Esta situación evidencia la necesidad de fortalecer y actualizar los mecanismos legales, técnicos e institucionales para garantizar una persecución penal eficaz de los ciberdelitos y una protección real de los bienes jurídicos tutelados en el entorno digital.

Capítulo 3

Los Niveles de Efectividad de los Mecanismos Usados para la Prevención de la Suplantación de Identidad.

En Colombia, a lo largo de los años, se han desarrollado diversos mecanismos normativos, jurisprudenciales e institucionales orientados a mitigar el fenómeno de la suplantación de identidad, conducta que pone en riesgo bienes jurídicos de especial relevancia como la identidad personal, el buen nombre y la seguridad de los sistemas financieros, electorales y administrativos del Estado. En este capítulo se analiza la efectividad de dichos mecanismos frente al delito de falsedad personal, particularmente en el contexto del uso de la inteligencia artificial como medio para su comisión.

Antes de la consolidación de un marco normativo especializado en protección de datos personales y tecnologías de la información, la Corte Constitucional ya había reconocido la gravedad de las consecuencias jurídicas derivadas de la suplantación de identidad. Un antecedente relevante se encuentra en la Sentencia T-455 de 1998, en la cual se estudió el caso del señor Fernando Téllez Lombana, quien fue víctima del hurto de sus documentos de identidad y, como consecuencia, suplantado por terceros durante varios años. Esta situación le generó antecedentes penales inexistentes, restricciones para salir del país y afectaciones profundas a su esfera personal y jurídica.

En dicho proceso, las decisiones adoptadas en primera y segunda instancia negaron la protección constitucional solicitada. No obstante, la Corte Constitucional revocó dichas providencias al considerar que se habían vulnerado los derechos fundamentales a la identidad, al buen nombre, a la honra y al hábeas data, reconociendo que el Estado tenía la obligación de garantizar la corrección y actualización de la información personal cuando esta fuera utilizada de manera indebida. Este pronunciamiento resulta especialmente significativo si se tiene en cuenta que para la época no existían aún leyes como la Ley 1266 de 2008 ni la Ley 1581 de 2012, que hoy regulan de manera expresa el tratamiento de los datos personales y establecen principios de seguridad, confidencialidad y veracidad.

Con la entrada en vigencia de la Constitución Política de 1991, el artículo 15 consagró la protección del derecho a la intimidad, al buen nombre y al hábeas data, lo que permitió posteriormente el desarrollo legislativo de estos derechos fundamentales. Sin embargo, el avance acelerado de la tecnología, particularmente de la inteligencia artificial, ha generado nuevas formas de afectación a la identidad personal que no se encontraban previstas en la regulación penal tradicional. En este contexto, la falsedad personal dejó de manifestarse únicamente a través de documentos físicos o actuaciones presenciales, para adoptar modalidades más complejas, como la creación de identidades falsas mediante imágenes, audios o videos generados artificialmente.

Frente a esta realidad, el legislador colombiano expidió la Ley 2502 de 2025, mediante la cual se modifica el artículo 296 del Código Penal, incorporando un agravante cuando el delito de falsedad personal se comete utilizando inteligencia artificial. Esta modificación representa un avance en el reconocimiento del impacto que tienen las nuevas tecnologías en la configuración de conductas delictivas, al aceptar que el uso de herramientas como los deepfakes incrementa el riesgo de daño, dificulta la identificación del autor y amplifica los efectos negativos sobre la víctima.

No obstante, la regulación adoptada no creó un tipo penal autónomo para las conductas realizadas mediante inteligencia artificial, sino que optó por agravar la sanción del delito ya existente. Desde una perspectiva de efectividad, esta decisión plantea interrogantes relevantes, pues si bien el agravante constituye un mecanismo disuasorio, su aplicación práctica depende de

la capacidad institucional para identificar, probar y judicializar el uso de inteligencia artificial en la comisión del delito. A la fecha, no se registran sentencias condenatorias en firme en las que se haya aplicado expresamente este agravante, lo cual se explica, en parte, porque la norma entra en plena vigencia a partir del año 2026 y aún se encuentra en fase de implementación.

En paralelo a la respuesta penal, el Estado colombiano ha adoptado medidas de carácter preventivo y administrativo orientadas a reducir la suplantación de identidad. Entre estas se destacan la implementación de la identificación biométrica en procesos electorales y la expedición de la cédula digital por parte de la Registraduría Nacional del Estado Civil. Estas herramientas fortalecen los mecanismos de verificación de identidad y disminuyen el margen de actuación de quienes intentan suplantar a otra persona, aunque no eliminan por completo los riesgos asociados al uso de tecnologías avanzadas.

Adicionalmente, Colombia ha fortalecido su marco de cooperación internacional mediante la adhesión al Convenio de Budapest sobre ciberdelincuencia, aprobado internamente por la Ley 1928 de 2018. Este instrumento ha permitido mejorar la capacidad del Estado para enfrentar delitos informáticos que trascienden las fronteras nacionales, facilitando el intercambio de información, la obtención de pruebas electrónicas y la identificación de los responsables. La firma del segundo protocolo complementario en 2022 refuerza aún más estos mecanismos, contribuyendo a una persecución penal más efectiva en contextos digitales.

A pesar de los avances normativos y tecnológicos, la experiencia colombiana evidencia que la regulación penal aún resulta insuficiente frente a los desafíos que plantea el uso de la inteligencia artificial en la comisión de delitos. La Ley 2502 de 2025 constituye un primer paso en el reconocimiento de esta problemática, pero la ausencia de tipos penales independientes y de una institucionalidad especializada limita la efectividad real de la respuesta estatal. En este sentido, se hace necesario avanzar hacia una legislación penal más específica y hacia la creación de entidades especializadas en delitos tecnológicos, que permitan una investigación más eficiente y una protección efectiva de los derechos fundamentales afectados por la suplantación de identidad mediante inteligencia artificial.

Conclusiones

A través de esta investigación se pudo concluir que, aunque Colombia no vaya a la par de la tecnología ha tenido avances significativos con la implementación de leyes que se encuentran en desarrollo. En Colombia hemos avanzado bastante con las soluciones biométricas (como las huellas, el reconocimiento facial y de voz). Estas sí funcionan, pero aun así no son difíciles de falsificar. Además, se ha podido evidenciar que en Colombia al pasar de los años los crímenes cibernéticos han tenido más alcances, vulnerando así mismos los derechos de las personas naturales y jurídicas. Uno de los avances más significativos fue implementar la identificación biométrica en un ámbito tan importante como es la registraduría nacional que tiene como principal objetivo registrar la vida civil de las personas, identificar a los ciudadanos y organizar los procesos electorales. Esto se hace para apoyar la administración de justicia y fortalecer la democracia del país una alternativa para ayudar a mitigar este problema es crear una ley que tenga como principal objetivo la inversión en infraestructura tecnología para fortalecer el marco legal de Colombia respecto a el delito de suplantación de identidad, que también incluya educación y capacitación fortaleciendo el sistema educativo en cuanto a la ciberseguridad en escuelas, universidades, entre otros. Esta ley debe tener normas claras y concisas que aporte en el fortalecimiento del vacío jurídico en Colombia en este momento, La cédula digital es mucho más segura que la antigua.

En atención a lo anterior, en la banca, estos sistemas han ayudado en gran manera a que no suplanten a las personas, haciendo uso de la doble verificación, en donde tener una clave no es suficiente, debes de registrar un número telefónico, un correo electrónico o en la mayoría de casos tener una aplicación móvil en donde cada cierto tiempo se genera una clave dinámica, todo con el fin de obtener una autenticación, lo cual hace que acceder a las cuentas bancarias sea menos probable. Por lo tanto, es mucho más complicado hacerse pasar por otra persona y lo más importante el agravante que se le ha dado al artículo 296 del código penal colombiano en donde el artículo 296 con su agravante es una de las herramientas legales más importantes que tiene hoy Colombia para:

- Proteger a los usuarios de portales bancarios y estatales.
- Castigar con más dureza a quienes afectan la confianza digital.

- Frenar el robo de datos a través de páginas o aplicaciones falsas.

Finalmente, puede establecerse un agravante a este tipo de delitos, lo cual deberá de reforzarse, crear nuevas políticas públicas en contra de la suplantación de identidad, quizás, creando un tipo penal independiente que tenga un contenido directo respecto a los delitos que se cometen en esta nueva era, pues no es suficiente sólo tener un agravante sobre un delito que ya no es cometido de forma tradicional, sino, que por medio de la tecnología se está perfeccionando cada vez más la delincuencia digital, lo que obliga a que deba integrarse en las leyes el manejo apropiado de cada una de estas conductas.

Referencias Bibliográficas

AESIA, https://aesia.digital.gob.es/es.

Ayllón, G.J. (2024). Inteligencia Artificial y Deepfakes: Las Ultrasuplantaciones Como Medio Para Vulnerar Los Derechos Al Honor, Intimidad Propia Imagen. Anuario de La Facultad de Derecho de La Universidad de Alcalá, 17, 3–32. https://doi.org/10.14679/3897 .

Benavides, E., Fuertes, W y Sánchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. https://revistas.uteq.edu.ec/index.php/cyt/article/download/357/407

Boté, V.J y Vállez, M. (2022). Aplicaciones de deepfakes. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad. Documentación de Las Ciencias de La Información, 45(1), 25–32. https://doi.org/10.5209/dcin.77256.

Cancillería. (2020). Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia. https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Cancillería. (2022). Colombia a la vanguardia de los procesos internacionales que buscan robustecer mecanismos para prevenir y perseguir el delito cibernético. https://www.cancilleria.gov.co/newsroom/news/colombia-vanguardia-procesos-internacionales-buscan-robustecer-mecanismos-prevenir

OpenAI. (2026). *ChatGPT* (versión GPT-4/5) [Modelo de lenguaje de inteligencia artificial]. https://chat.openai.com/

Cañas, Q.M., Cuellar, O.A y Marín, A.A. (2021). Delitos informáticos que afectan a los consumidores financieros del banco Davivienda. Fundación Universitaria Los Libertadores. Bogotá. https://repository.l

ibertadores.edu.co/server/api/core/bitstreams/30b5cbaf-fe65-4335-bb72-4f9b7d70a22c/content

Congreso de la República de Colombia. (2008). Ley 1266 de 2008. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2012). Decreto 2364 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2012). Ley Estatutaria 1581 de 2012.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2017). Decreto 1413 de 2017.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83253.

Congreso de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587. El Gobierno Nacional radicó al Congreso de la República el Proyecto de Ley para adherirse al tratado internacional, que tiene como objetivo hacer frente a los delitos informáticos y en Internet mediante la cooperación entre las naciones. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/56315:Gobierno-radico-Proyecto-de-Ley-para-adherirse-al-Convenio-de-Budapest-contra-la-ciberdelincuencia.

Congreso de Colombia. (2014). Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficial No. 49.084 del 6 de marzo de 2014.https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes%2F1687091

Congreso de Colombia. (2018). Ley 1928 de 2018: Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Diario Oficial No. 50.664. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes%2F30035501

Congreso de la República de Colombia, Cámara de Representantes. (2021). "Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de Inteligencia Artificial y se dictan otras disposiciones". https://www.camara.gov.co/sites/default/files/2021-10/P.L.354-2021C%20%28INTELIGENCIA%20ARTIFICIAL%29.pdf

Congreso de la República de Colombia. (2024). *Por medio del cual se modifica y establece un agravante al artículo 296 de la Ley 599 de 2000 Código Penal Colombiano* [Proyecto de Ley 225 de 2024 Cámara]. Cámara de Representantes. https://www.camararep.gov.co/documento/proyecto-de-ley-225-de-2023-camara-0

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2025). *Ley 2502 de 2025. Por medio de la cual se…* Ley 2502 de 2025 Modifica y establece un agravante en el Código Penal por el uso de la Inteligencia Artificial. Rama Judicial. https://sidn.ramajudicial.gov.co/SIDN/DOCTRINA/TEXTOS_COMPLETOS/infografias/Leyes/2025/Ley_2502_2025.html

Consejo de Europa. (2023). *Convenio sobre la ciberdelincuencia (STE n.º 185): Informe explicativo y notas de orientación; Protocolo sobre la xenofobia y el racismo; Segundo protocolo adicional relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas*. Consejo de Europa. https://www.coe.int/cybercrime

Convenio de Budapest. (2001). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Constitución Política de Colombia. (1991). Diario Oficial No. 109.465 del 4 de julio de 1991. Art.21. https://www.constitucioncolombia.com

Continuum GRC. (2023). Cifrado biométrico y protección de datos personales. https://continuumgrc.com/es/biometric-encryption-and-protecting-personal-data/

Corredor, B.D (2022). Resolución sobre demanda de la casación y doble conformidad. SP592-2022 Radicación 50621. Acta 43.Bogotá D.C.: Corte Suprema de Justicia https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2022/SP592-2022(50621).pdf

Corte Constitucional de Colombia, Sala Segunda de Revisión. (1998). Sentencia T-455/98. Magistrado Ponente: Antonio Barrera Carbonell.

Corte Constitucional de Colombia, Sala Sexta de Revisión. (2022). Sentencia T-8.727.419. Magistrado ponente: Hernán Correa Cardozo.

https://drive.google.com/drive/folders/1zTSWJyDxe4Pa6ituGlSg0XObcItlLD2U

Cortez, M.K., Uribe, M.A., Lopera, M.M., Aristizábal, S.S., Ramírez, B.C. et al. (2023). Por medio de la cual se define y regula la inteligencia artificial, se establecen límites frente a su desarrollo, uso e implementación y se dictan otras disposiciones. https://www.camara.gov.co/inteligencia-artificial-1.

Corte Suprema de Justicia. (2022, abril 25). Sentencia SC712-2022. Sala de Casación Civil.https://www.hklaw.com/en/insights/publications/2022/07/corte-suprema-de-justicia-se-pronuncia-sobre-la-prescripcion.

CSIRT (s. f). Ciber consejos para protegerse del RANSOMWARE.Ministerio del Interior y Salud Pública. Chile.https://anci.gob.cl/documents/4532/Ciberconsejos-ransomware.pdf.

Díaz, S.G., Molina, G.A y Serrador, O.L (2023). Aproximación al ciberdelincuente desde la perspectiva del control social. Revista Criminalidad, 65(3), 81-95. Epub March 09, 2024. https://doi.org/10.47741/17943108.508.

Dirección de Cómputo y Comunicaciones, s.f.). Deepfake. Instituto Técnico Nacional. https://www.seguridad.ipn.mx/comunicados/Infografia_Deepfake.pdf.

De los Monteros Pérez-Brotóns, S. E., & Sanz Setién, G. (2024). El Reglamento De Ia: El Primer Paso Del Camino Hacia Una Regulación Completa De La Inteligencia Artificial. Actualidad Jurídica (1578-956X), 65, 180–196.

Echavarría, S.J., Correal, H.F., Arias, F.J., Rodríguez, P.C., Benedetti, M.J. et al. (2021). Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de Inteligencia Artificial y se dictan otras disposiciones. https://www.camara.gov.co/inteligencia-artificial-0.

España. (1995). *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Boletín Oficial del Estado, núm. 281, de 24 de noviembre de 1995.

Fiscalía General del Estado. (2023). *Memoria de la Fiscalía General del Estado 2023*.https://www.fiscal.es/memorias/memoria2023/FISCALIA_SITE/index.html IA DeepSeek

Franganillo, J. (2023). La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos. methaodos.Revista De Ciencias Sociales, 11(2), m231102a10. https://doi.org/10.17502/mrcs.v11i2.710

Fernández, A., Fernández, D., Molero, D., Pérez, M., García, B. et al. (2025). DEEPFAKES: RIESGOS, CASOS REALES Y DESAFÍOS EN LA ERA DE LA IA. https://www.ismsforum.es/ficheros/descargas/deepfake-final1742458135.pdf.

Fernández, G.J (2007). Encriptación y Desencriptación de Datos Usando Técnicas caóticas. [Tesis de Maestría]. Universidad Nacional de Colombia. Manizales. https://repositorio.unal.edu.co/bitstream/handle/unal/7079/josearmandofernandezgallego.2007.pdf?sequence=1&isAllowed=y.

Garriga Domínguez, A. (2024). Los Derechos Ante Los Sistemas Biométricos Que Incorporan Inteligencia Artificial. Revista Derechos y Libertades, 51, 117–149. https://doi.org/10.20318/dyl.2024.8585

Jiménez Serranía, V., Calderón Marenco, E. A., Agón López, J. G., & Ravelo Franco, G. (2025). La regulación de la inteligencia artificial: la complejidad en la búsqueda de un equilibrio de intereses. Especial foco en la protección de la creación y de la innovación. Visión comparada UE-Colombia. Dixi, 27, 1–23. https://doi.org/10.16925/2357-5891.2025.03.09

Ministerio del Interior. (2023). *Informe sobre seguridad ciudadana 2023*.

https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2023/balance-de-seguridad-ciudadana-2023 DeepSeek IA

Martínez Galindo, G. (2024). Suplantación de identidad digital: hacia una necesaria tutela penal . Estudios De Deusto, 72(1), 199-228. https://doi.org/10.18543/ed.3105

Medina, G.A. (2013). Panorama de biometría dactilar en Colombia. Universidad Piloto de Colombia. Bogotá. https://repository.unipiloto.edu.co/handle/20.500.12277/2608?show=full

Mendoza, R.L (2022). La imagen como forma de (des)conocimiento en la era del deepfake. ANIAV - Revista De Investigación En Artes Visuales, (11), 53–70. https://doi.org/10.4995/aniav.2022.17309.

Ministerio para la Transformación Digital y de la Función Pública. (2025, 11 de marzo). *El Gobierno da luz verde al anteproyecto de ley para un uso ético, inclusivo y beneficioso de la inteligencia artificial* [Nota de prensa]. Gobierno de España. https://www.digital.gob.es/…

Ministerio para la Transformación Digital y de la Función Pública. (2025). El Gobierno da luz verde al anteproyecto de ley para un uso ético, inclusivo y beneficioso de la Inteligencia Artificial.

Mitek (s.f). Biometría de voz: qué es y cómo funciona.

https://www.miteksystems.com/es/blog/biometria-voz-nueva-tecnologia#:~:text=%C2%BFQu%C3%A9%20es%20la%20biometr%C3%ADa%20de,alguien%20es%20quien%20dice%20ser.

Presidencia de la República de Colombia (2017). Decreto 1413 de 2017: Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Diario Oficial No. 50.339. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30033063.

Pulgarin, B.J., Echavarría, S.J., Arias, F.J., Muñoz, C.F., Acosta, L.C. et al. (2020).

"Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de Inteligencia Artificial y se dictan otras disposiciones". https://www.camara.gov.co/inteligencia-artificial.

¿Qué es el smishing (phishing por SMS)? (2024, octubre 24). Ibm.com. https://www.ibm.com/mx-es/topics/smishing

RedesZone. (2024). Qué es Web Spoofing y cómo protegernos de estos ataques. https://www.redeszone.net/tutoriales/seguridad/que-es-web-spoofing/

Registraduría Nacional del Estado Civil. (2024). Cédula digital colombiana.

https://www.registraduria.gov.co/-Cedula-de-ciudadania-digital-1616-.html

de Publicaciones de la Unión Europea, O., & Luxemburgo, L. (n.d.). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)Texto pertinente a efectos del EEE.* http://data.europa.eu/eli/reg/2024/1689/oj

Rojas, P.A. y Suárez, R.J. (2018). La huella dactilar como mecanismo de identificación biométrica para la no portabilidad de documentos de identidad. TIA, 6(2), pp. 38-44.https://revistas.udistrital.edu.co/index.php/tia/article/download/12761/14691

Senado de la República de Colombia. (2017). Proyecto de Ley 058 de 2017. https://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2017-2018/898-proyecto-de-ley-058-de-2017

Senado de la República de Colombia. (2022). Proyecto de Ley 253 de 2022. https://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2022-2024/2840-proyecto-de-ley-253-de-2022 P 1-17

Senado de la República de Colombia. (2023). Proyecto de Ley 200 de 2023. Por la cual se define y regula la inteligencia artificial, se ajusta a estándares de derechos humanos, se establecen límites frente a su desarrollo, uso e implementación se modifica parcialmente la ley 1581 de 2012 y se dictan otras disposiciones. https://www.camara.gov.co/inteligencia-artificial-1.

Senado de la República de Colombia. (2025). Proyecto de Ley 043 de 2025. "Por medio de la cual se regula la Inteligencia Artificial en Colombia para garantizar su desarrollo ético, responsable, competitivo e innovador, y se dictan otras disposiciones". https://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2025-2026/3569-proyecto-de-ley-043-de-2025.

SEON, (s.f). Deepfake. ¿Qué son los deepfakes? https://seon.io/es/recursos/glosario/deepfake/.

Serrano, C. (2023). Retina, Globo ocular. Kenhub. https://www.kenhub.com/es/library/anatomia-es/retina-es.

Sistema Nacional de Bibliotecas Judiciales. (2018). Ley 1928 de 2018. https://sidn.ramajudicial.gov.co/SIDN/NORMATIVA/TEXTOS_COMPLETOS/7_LEYES/LEYES%202018%20(1877-)/Ley%201928%20de%202018%20(Aprueba%20el%20Convenio%20sobre%20Ciberdelincuencia).pdf

SURA (s.f). Datos biométricos. Centro de protección digital. https://www.segurossura.com.co/documentos/centro-proteccion-digital/datos-biometricos.pdf.

Tarlogic Security. (2023). Así funciona el shimming y así puedes evitarlo. https://www.tarlogic.com/es/blog/shimming-como-funciona-evitarlo/

Tribunal Superior de Medellín, Sala de Decisión Penal. (2022). Proceso No. 053606099057 2021-50679. https://salapenaltribunalmedellin.com/images/pdf/providenciaspenal/030/05360609905720215067 9.pdf

Utimaco. (s. f.). ¿Qué es la criptografía asimétrica? Utimaco. pág. s. p. https://utimaco.com/es/servicio/base-de-conocimientos/gestion-de-claves-y-secretos/que-es-la-criptografia-asimetrica

Visus, A. (2021). ¿Qué es un Deep fakes, cómo se crean, cuáles fueron los primeros y su futuro? https://www.esic.edu/rethink/tecnologia/deep-fakes-que-es-como-se-crean-primeros-y-futuros