

EL USO DE LA INTELIGENCIA ARTIFICIAL EN LA FALSEDAD PERSONAL: UN NUEVO
DESAFIO PARA EL DERECHO PENAL COLOMBIANO



JUAN ESTEBAN MEJIA VERGARA

UNIVERSIDAD SANTIAGO DE CALI

TRABAJO DE GRADO PRESENTADO PARA OPTAR AL TITULO DE ABOGADO

DIPLOMADO EN DERECHO PENAL Y PROCESAL PENAL

FACULTAD DE DERECHO

TUTORA: JINNETH ELENA GAVIRIA GAVIRIA

MAYO, 2025

El vertiginoso avance tecnológico y la creciente integración de sistemas de inteligencia artificial en diversas esferas sociales han generado nuevos desafíos para el derecho penal, particularmente en lo concerniente a la suplantación de identidad o falsedad personal. En el contexto colombiano, donde la modernización de los procesos judiciales y la digitalización de la información han ido en paralelo con la aparición de delitos cibernéticos, se hace indispensable revisar y adaptar el marco jurídico vigente para responder de manera eficaz a conductas delictivas que, por su complejidad, trascienden los límites de las normas tradicionales, en consonancia con la perspectiva integradora que demanda el estudio de los fenómenos delictivos contemporáneos. La formulación de estrategias que fortalezcan la respuesta del sistema penal colombiano ante las conductas ilícitas derivadas del uso de la inteligencia artificial tiene como finalidad articular propuestas de reforma que combinen el análisis normativo, criminológico y procesal, en aras de consolidar un marco jurídico robusto y adaptable a los retos de la era digital.

La problemática que se aborda en este ensayo se encuentra inmersa en el siguiente interrogante: ¿Cómo impacta el uso de la inteligencia artificial en la falsedad personal y qué desafíos representan para la regulación y aplicación del derecho penal colombiano?

Así, surge como fin analizar el marco normativo penal colombiano frente a los desafíos emergentes. En este orden, se evalúa las implicaciones criminológicas y procesales de la inteligencia artificial en la comisión de delitos. Finalmente, se desarrollan estrategias integradoras para el fortalecimiento del derecho penal en contextos tecnológicos.

El análisis doctrinal y jurisprudencial se configura como eje central de este estudio, pues resulta imperativo identificar los vacíos y desafíos que plantea la utilización de tecnologías avanzadas en la perpetración de delitos de suplantación de identidad. En este sentido, el ensayo tiene como propósito principal examinar cómo las disposiciones legales y reglamentarias vigentes

se adaptan o requieren adaptación para abordar esta problemática, considerando la evolución de la doctrina penal y la tendencia de los pronunciamientos judiciales en casos análogos (García, 2018).

A partir de una metodología cualitativa con enfoque socio jurídico, el estudio busca no solo comprender la naturaleza y magnitud del problema, sino también proponer soluciones viables y coherentes con los principios fundamentales del derecho penal y los desafíos que plantea la modernidad tecnológica. Abarcando desde la revisión del marco normativo hasta el estudio de los impactos criminológicos y procesales derivados del uso indebido de la inteligencia artificial en la comisión de delitos, constituyendo así una propuesta integral que busca sentar las bases para una reforma del sistema penal colombiano en esta modalidad.

El análisis del marco normativo penal colombiano revela que los preceptos sobre falsedad personal se formularon antes de la explosión de la inteligencia artificial como herramienta de creación masiva de contenidos sintéticos, por lo que su referencia a imagen y voz permanece anclada a soportes físicos o a archivos con firma digital reconocida (Congreso de la República de Colombia, 2000). La doctrina mayoritaria interpreta que debe existir un “documento” formal para subsumir la conducta, excluyendo los deepfakes generados en tiempo real sin formato contractual o registro (Martínez, 2024). Este enfoque materialista contrasta con la Convención de Budapest, que ya en 2001 agravó la falsedad cometida por medios electrónicos sin exigir documento físico y con la propuesta de directiva de la Comisión Europea de 2023, que tipifica la manipulación algorítmica de audio y video como infracción grave (Naranjo Hincapié, 2023).

Al examinar proyectos de ley radicados en el Congreso colombiano entre 2020 y 2024, se observa que solo se proponen penas generales para delitos informáticos sin diferenciar la sofisticación técnica de la IA ni definir contenido sintético (Ámbito Jurídico, 2024). Autores

como Sanabria (2024) han subrayado que sin una definición legal de huella algorítmica y firma generativa adversaria, los peritos carecen de marco para certificar la autoría de un deepfake y los fiscales deben recurrir a analogías imprecisas. Además, al no existir un agravante específico por el uso de IA, se aplica la misma pena a un fraude rudimentario y a un ataque masivo automatizado, lo que vulnera el principio de proporcionalidad (Regueiro, 2023).

En la era digital, la suplantación de identidad ha trascendido las formas tradicionales de fraude, adoptando nuevas modalidades facilitadas por tecnologías emergentes como la inteligencia artificial (IA). En particular, la utilización de técnicas de deepfake ha permitido la creación de contenidos audiovisuales hiperrealistas que pueden ser empleados para imitar la apariencia y voz de personas reales, con fines maliciosos (Santos, 2017). Esta evolución tecnológica plantea desafíos significativos para el sistema penal colombiano, tanto en términos criminológicos como procesales.

Desde una perspectiva criminológica, la suplantación de identidad mediante IA representa una amenaza creciente que afecta la confianza en las interacciones digitales y la integridad de la información. Los delincuentes pueden utilizar *deepfakes* para difundir información falsa, manipular opiniones públicas o cometer fraudes financieros, entre otras actividades ilícitas. La facilidad con la que se pueden crear estos contenidos y su realismo dificultan la detección por parte de las víctimas y las autoridades, lo que incrementa la impunidad y la sofisticación de las conductas delictivas (Centro de Estudios Regulatorios, 2022).

Además, la naturaleza transnacional de internet permite que estos delitos se cometan desde cualquier parte del mundo, complicando la jurisdicción y la cooperación internacional en la persecución penal. La anonimidad que ofrece el ciberespacio también dificulta la identificación de los responsables, lo que requiere de estrategias de investigación más avanzadas y

colaborativas entre diferentes países y organismos internacionales (Martínez, 2024). En el ámbito procesal, la introducción de pruebas generadas por IA plantea interrogantes sobre su autenticidad y admisibilidad en los procesos judiciales. La manipulación de imágenes y sonidos mediante deepfakes puede generar evidencias falsas que, si no son correctamente identificadas, podrían influir en las decisiones judiciales y comprometer la justicia. Esto exige el desarrollo de capacidades técnicas y periciales especializadas que permitan verificar la veracidad de los contenidos digitales presentados como prueba (Centro de Estudios Regulatorios, 2022).

Asimismo, el uso de herramientas de IA por parte de las autoridades judiciales debe ser regulado para garantizar el respeto al debido proceso y los derechos fundamentales de las personas. La Corte Constitucional de Colombia ha señalado que, aunque la IA puede ser utilizada como apoyo en la administración de justicia, no debe sustituir la función de los jueces humanos ni comprometer la transparencia y la responsabilidad en la toma de decisiones (Corte Constitucional, 2024).

Frente a estos desafíos, es imperativo que el sistema penal colombiano adopte una respuesta integral que incluya la actualización de las normas penales para tipificar adecuadamente los delitos cometidos mediante IA, el fortalecimiento de las capacidades técnicas y humanas de las autoridades judiciales y la promoción de la cooperación internacional en la lucha contra la criminalidad digital. Además, es fundamental fomentar la educación y la concienciación pública sobre los riesgos asociados al uso indebido de la IA, para prevenir la victimización y promover un uso ético y responsable de las tecnologías emergentes (Corte Constitucional, 2024).

En la actualidad, la inteligencia artificial (IA) ha modificado sustancialmente el ecosistema delictivo. La irrupción de herramientas que simulan voz, imagen, movimiento facial e

incluso escritura con grados de realismo nunca alcanzados ha dado paso a nuevas tipologías criminales, entre las cuales la suplantación de identidad ocupa un lugar prioritario por su potencial afectación a bienes jurídicos fundamentales como la intimidad, la honra, la seguridad jurídica, el patrimonio y la libertad de decisión (Regueiro, 2023). Frente a este fenómeno, se hace imprescindible un análisis que abarque tanto la dimensión criminológica, es decir, cómo y por qué se produce esta forma de delito en el entorno digital como la procesal, que debe encargarse de esclarecer cómo puede y debe responder el sistema judicial a tales desafíos de forma eficaz y garantista.

Desde el plano criminológico, se debe entender que los delitos de suplantación de identidad han evolucionado desde prácticas rudimentarias, como el uso de documentos falsificados o la usurpación de datos personales por medios análogos, hacia formas complejas de criminalidad tecnológica donde el agresor no necesita presencia física ni interacción directa con la víctima (Centro de Estudios Regulatorios, 2022). Gracias a redes generativas adversarias, los agresores pueden crear en minutos una representación visual o sonora falsa de una persona específica, incluso a partir de una mínima cantidad de información tomada de redes sociales. Este nuevo tipo de delincuente frecuentemente anónimo, geográficamente remoto y altamente tecnificado configura lo que algunos doctrinantes han denominado una criminalidad algorítmica cuyas características principales son la automatización, la anonimización y la escalabilidad de la conducta (Naranjo Hincapié, 2023).

A diferencia del delincuente tradicional, el sujeto activo de la suplantación digital no necesariamente responde a motivaciones económicas directas. Puede actuar por lucro, pero también por fines políticos, reputacionales, ideológicos o incluso por mero entretenimiento (lo que se conoce en el lenguaje de internet como *trolling*). La multiplicidad de móviles y la facilidad

para diseminar los contenidos generados complica la labor de persecución penal, pues los daños se producen en cadena, con efectos en múltiples víctimas y múltiples jurisdicciones. Asimismo, el impacto criminológico de estos delitos suele ser subestimado, dado que no siempre dejan una huella física o inmediata, pero sí pueden arruinar reputaciones, destruir vínculos laborales o familiares, generar secuelas psicológicas e incluso llevar al suicidio de las víctimas, como lo han documentado estudios recientes sobre violencia digital en Latinoamérica (Martínez, 2024).

En el ámbito procesal, los retos son igualmente profundos. Uno de los principales problemas radica en la obtención y valoración de la prueba. Cuando un contenido sintético es presentado como evidencia, el fiscal o el defensor deben determinar si es auténtico, si ha sido manipulado o si fue completamente fabricado por un algoritmo. Las herramientas tradicionales de análisis forense digital que buscan metadatos, firmas digitales o estructuras de codificación resultan insuficientes frente a contenidos creados desde cero por IA. Por ello, se requiere incorporar métodos más sofisticados, como el análisis de patrones de entrenamiento de modelos generativos, la reconstrucción de “huellas algorítmicas” o la detección de artefactos visuales invisibles al ojo humano, pero identificables por inteligencia artificial forense (Sanabria, 2024).

No menos importante es la tensión entre el uso legítimo de IA como herramienta investigativa y la protección de los derechos fundamentales del procesado. En Colombia, el debido proceso penal consagrado en el artículo 29 de la Constitución Política exige que las pruebas sean obtenidas legalmente, valoradas por un juez imparcial y refutables por la defensa (Ministerio de Justicia y del Derecho, 2019). Sin embargo, cuando la Fiscalía utiliza software de reconocimiento facial, análisis predictivo o rastreo automatizado sin control judicial, se abre la puerta a posibles violaciones de la presunción de inocencia y del derecho a la defensa. Además, muchos de estos algoritmos operan como “cajas negras”, es decir, no permiten conocer los

criterios de decisión interna que usan para emitir un resultado. Si un ciudadano es vinculado a un proceso penal a partir de una coincidencia algorítmica que no puede ser auditada ni comprendida por peritos humanos, el principio de contradicción se ve seriamente comprometido (Corte Constitucional, 2024).

Otro problema procesal relevante es la preservación de la cadena de custodia digital. A diferencia de un documento físico, los archivos electrónicos pueden ser duplicados, modificados o destruidos con facilidad, sin dejar rastro aparente. Cuando se trata de evidencias generadas por IA, este riesgo se multiplica, ya que es posible alterar un contenido sin afectar su metadata, engañando incluso a softwares forenses. De ahí que resulte fundamental desarrollar protocolos actualizados de manejo de evidencia algorítmica, que incluyan sellado criptográfico, marcas digitales de procedencia, validación mediante blockchain y control de integridad por entes externos especializados (Sanabria, 2024).

Además, la labor de los peritos judiciales debe ser repensada: ya no basta con tener conocimientos en informática forense clásica. Es indispensable que los peritos penales en estos casos tengan formación en ciencia de datos, arquitectura de redes neuronales, teoría de la información y seguridad cibernética. Igualmente, los jueces deben estar capacitados para comprender el funcionamiento básico de estas tecnologías, evaluar la fiabilidad de los informes técnicos y tomar decisiones informadas que resguarden los derechos de todas las partes (Corte Constitucional, 2024).

En este escenario, la capacitación es una herramienta indispensable. Tanto fiscales como jueces y defensores deben actualizarse de manera permanente en tecnologías emergentes y sus aplicaciones jurídicas. Esta actualización debe ir de la mano con la construcción de una doctrina nacional que integre criterios interpretativos sobre la validez de las pruebas digitales, la

responsabilidad penal en contextos algorítmicos y la determinación de la autoría en delitos cometidos sin intervención humana directa. Así como en su momento el derecho penal se adaptó a los delitos cometidos con armas de fuego, vehículos motorizados o sustancias químicas, hoy debe dar un paso similar con la inteligencia artificial (Santos, 2017).

Por ende, el uso de IA en la suplantación de identidad exige una revisión profunda de las categorías criminológicas y procesales tradicionales. Las instituciones del Estado deben fortalecer su capacidad técnica, legislativa y humana para enfrentar un tipo de criminalidad que no solo es invisible y descentralizada, sino también en constante evolución (Corte Constitucional, 2024). Solo una respuesta articulada, ética y científicamente informada podrá garantizar que el derecho penal colombiano no quede anclado en el siglo XX mientras el delito ya avanza en la segunda mitad del siglo XXI.

La acelerada expansión del uso de la inteligencia artificial (IA) en contextos civiles y comerciales ha generado un entorno de alta sofisticación que, en manos inadecuadas, se transforma en un escenario propicio para la perpetración de nuevas conductas delictivas. Entre ellas, la suplantación de identidad a través de herramientas como deepfakes representa uno de los mayores desafíos para el derecho penal colombiano contemporáneo. Frente a esta realidad, se requiere una respuesta estratégica multidimensional que combine elementos normativos, institucionales, educativos y técnicos. Tales respuestas no solo deben centrarse en el castigo posterior al delito, sino también en su prevención, detección temprana y neutralización dentro del marco constitucional (Corte Constitucional, 2024).

Desde el plano normativo, es imprescindible la tipificación de una conducta autónoma que reconozca la gravedad de la suplantación de identidad mediante herramientas algorítmicas, como una modalidad delictiva de falsedad personal de nueva generación. Este tipo penal debe

contener elementos objetivos y subjetivos que identifiquen claramente el uso de IA como mecanismo para alterar o falsear una identidad ajena. Asimismo, se propone la introducción de un **agravante específico** en los artículos 292 y 293 del Código Penal, que incremente las penas cuando el hecho sea cometido mediante la generación de contenido sintético audiovisual o textual producido por algoritmos de aprendizaje automático (Sanabria, 2024). Este tipo de agravantes ya ha sido aplicado en modelos normativos de países como Alemania, Canadá y Japón, donde la sofisticación del medio comisivo es considerada un factor que incrementa la lesividad social del hecho (Regueiro, 2023).

Además, se hace urgente la reforma del Código de Procedimiento Penal colombiano, con la finalidad de introducir protocolos claros para la recolección, análisis y admisión de pruebas digitales generadas o alteradas por inteligencia artificial. Dichos protocolos deben contemplar la participación de peritos informáticos especializados en redes generativas, así como métodos de validación cruzada para evitar falsos positivos y garantizar el respeto al debido proceso. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con la fiscalía general de la Nación, podría ser el órgano rector encargado de certificar herramientas de detección de deepfakes, de establecer estándares nacionales de autenticidad digital y de desarrollar una base de datos que registre “huellas algorítmicas” detectadas en contextos penales (Ámbito Jurídico, 2024).

Complementariamente, se sugiere la consolidación de tribunales tecnológicos especializados en delitos informáticos, integrados por jueces con formación en ética de la inteligencia artificial, derecho digital y técnicas probatorias aplicadas a evidencias no estructuradas. La capacitación continua del personal judicial en estas áreas será clave para garantizar decisiones fundadas, justas y técnicamente acertadas (Santos, 2017). En esta línea, el

Consejo Superior de la Judicatura podría implementar diplomados obligatorios para los jueces de las salas penales, con contenidos desarrollados en alianza con universidades y centros de innovación tecnológica.

Desde el enfoque de la prevención, resulta crucial incorporar una estrategia educativa que promueva la alfabetización digital avanzada en el sistema educativo colombiano. Esta alfabetización no debe limitarse al uso básico de herramientas digitales, sino que debe enseñar a la ciudadanía, desde la educación media, a identificar señales de manipulación algorítmica, a comprender los riesgos de compartir información personal sin filtros, y a reconocer las formas contemporáneas de fraude digital. Se propone la creación de módulos pedagógicos diseñados por el Ministerio de Educación Nacional, con el apoyo de universidades, y su integración en los programas de ética y tecnología de instituciones públicas y privadas (Ministerio de Justicia y del Derecho, 2019).

En el ámbito de las políticas públicas, se hace fundamental el desarrollo de alianzas estratégicas con el sector privado, en especial con las empresas tecnológicas proveedoras de redes sociales, motores de búsqueda y servicios en la nube. A través de convenios interinstitucionales, estas compañías pueden colaborar en el desarrollo de herramientas automatizadas de detección de contenido falso, y en la implementación de sellos de verificación digital basados en blockchain, que garanticen la autenticidad e integridad de los datos compartidos por los usuarios. Esta propuesta se fundamenta en los principios de corresponsabilidad social y ética tecnológica, en los que los desarrolladores de tecnologías asumen parte del deber de prevenir su mal uso (Naranjo Hincapié, 2023).

El ordenamiento jurídico penal colombiano se ha mantenido, en su estructura fundamental, relativamente estable durante las últimas dos décadas. No obstante, la evolución

exponencial de las tecnologías de información y comunicación ha provocado una disonancia entre la velocidad del cambio técnico y la capacidad de adaptación del sistema legal. Uno de los ámbitos donde esta brecha es más evidente es en la regulación de las conductas que implican la suplantación de identidad mediante inteligencia artificial (IA), fenómeno que exige una revisión profunda del marco normativo vigente para responder eficazmente a nuevos escenarios delictivos (Corte Constitucional, 2024).

El delito de falsedad personal, regulado en los artículos 292 y 293 del Código Penal colombiano (Ley 599 de 2000), contempla como conducta punible la suplantación de identidad, ya sea por medios directos o mediante el uso de nombres, documentos o signos que representen a una persona sin su consentimiento. Esta figura jurídica se diseñó para enfrentar casos concretos de usurpación en trámites notariales, judiciales o administrativos, en un contexto en el que los delitos informáticos apenas comenzaban a adquirir protagonismo. En ese sentido, el legislador no previó ni conceptual ni técnicamente la posibilidad de que existieran tecnologías capaces de replicar rostros, voces, gestos e incluso personalidades humanas con un grado de fidelidad tan alto que resultara prácticamente imposible distinguir entre lo falso y lo real (Congreso de la República de Colombia, 2000).

La emergencia de herramientas como los deepfakes, que utilizan redes generativas adversarias para crear contenido sintético hiperrealista, ha trastocado la manera en que debe entenderse la “identidad” en el plano jurídico. Estas tecnologías permiten que una persona pueda ser representada, sin su conocimiento ni autorización, en imágenes o grabaciones que simulan acciones o declaraciones falsas (Superintendencia de Industria y Comercio, 2022). Tal manipulación no solo atenta contra su dignidad, sino que además plantea serios riesgos en contextos como procesos judiciales, campañas políticas, fraudes económicos y extorsiones. Sin

embargo, en Colombia, no existe aún un tipo penal que contemple de forma específica estas nuevas formas de afectación a la identidad, lo cual genera impunidad o dificulta la subsunción típica en las normas existentes (Sanabria, 2024).

En la jurisprudencia colombiana, se ha consolidado un criterio interpretativo que exige que la falsedad se materialice sobre “documentos” con algún grado de formalidad o estructura, incluso cuando se trata de soportes informáticos. Por ejemplo, de acuerdo con la Corte Suprema de Justicia, se sostuvo que para que exista falsedad en documento, debe demostrarse la existencia de una alteración fraudulenta sobre un contenido previamente existente, lo cual excluye los casos en que el contenido fue fabricado desde cero por medios tecnológicos (Corte Suprema de Justicia, 2020). Esta visión excluye del tipo penal las situaciones donde un deepfake genera una identidad completamente inventada, pero visualmente atribuible a una persona real.

Además, la interpretación tradicional del tipo penal de falsedad personal carece de un componente subjetivo que contemple la intención dolosa ampliada mediante el uso de IA. En otras palabras, el legislador no ha diferenciado entre el engaño artesanal y el engaño potenciado tecnológicamente, lo cual impide sancionar con mayor severidad a quienes, usando IA, logran realizar ataques masivos y con alto potencial de daño reputacional, financiero o psicológico (Ministerio de Justicia y del Derecho, 2019).

El escenario internacional revela que algunos países han empezado a llenar estos vacíos legales. En Francia, por ejemplo, se establece como delito la difusión de contenido manipulado por inteligencia artificial que pueda alterar el orden público o afectar la imagen de una persona pública. En Estados Unidos, estados como California han aprobado normas que criminalizan la creación y difusión de deepfakes con fines de manipulación política o fraude electoral, especialmente en contextos electorales (Naranjo Hincapié, 2023). En ambos casos, la ley

reconoce que el uso de IA no es un simple medio neutral, sino un potenciador de capacidades ilícitas que debe ser contemplado por el derecho penal como una agravante o incluso como un tipo penal autónomo.

Frente a ese panorama, el derecho penal colombiano debe asumir una transformación urgente. Por un lado, es necesario actualizar la definición de “documento” y “suplantación de identidad” en el Código Penal, de manera que se incluya expresamente cualquier contenido generado mediante algoritmos de aprendizaje profundo o inteligencia artificial generativa. Esta modificación debe reflejar el carácter intangible de los nuevos medios comisivos, superando la visión tradicional que se enfoca exclusivamente en el soporte físico o digital con formato estructurado. Por otro lado, resulta prioritario diseñar un tipo penal autónomo de “suplantación algorítmica de identidad” que incluya como elementos típicos: (i) la utilización de sistemas de IA para imitar o falsificar la apariencia, voz o comportamiento de otra persona; (ii) la intención de engañar, difamar, extorsionar, obtener lucro o cualquier otro fin ilícito; y (iii) la posibilidad de causar un daño tangible o intangible a la víctima, ya sea en su reputación, patrimonio, intimidad o integridad psicosocial (Martínez, 2024).

Esta nueva figura penal no solo reforzaría la capacidad sancionatoria del Estado, sino que también cumpliría una función preventiva, al enviar un mensaje claro de intolerancia frente a este tipo de manipulaciones. Además, permitiría establecer diferencias punitivas más justas entre quien comete una suplantación sencilla y quien utiliza tecnología de punta para generar un daño masivo y potencialmente irreversible. Tal distinción sería coherente con el principio de proporcionalidad de la pena y con el mandato constitucional de protección de la dignidad humana.

No debe olvidarse que la modernización del derecho penal frente a la inteligencia artificial también requiere de una revisión en clave garantista. Cualquier tipo penal nuevo debe establecer con claridad los elementos objetivos y subjetivos de la conducta, respetar el principio de legalidad y prever mecanismos de defensa técnica adecuados. En este sentido, el desarrollo doctrinal debe acompañar la legislación, promoviendo una teoría del delito adaptada a los entornos digitales, sin caer en expansiones indebidas del ius puniendi que comprometan libertades fundamentales. Así lo ha advertido la Corte Constitucional colombiana, al recordar que la criminalización de nuevas conductas debe ser excepcional, necesaria y respetuosa de los principios rectores del Estado de derecho (Corte Constitucional, 2024).

Resulta pertinente establecer un observatorio nacional sobre inteligencia artificial y delito, que actúe como órgano asesor del Estado en materia de riesgos tecnológicos, evolución del crimen digital y elaboración de políticas públicas. Este observatorio, además de realizar estudios prospectivos, puede articular una red de colaboración internacional que permita compartir conocimientos y experiencias exitosas con organismos como Europol, Interpol, la ONU y agencias especializadas en ciberseguridad. Así, Colombia podrá anticiparse a nuevas formas de criminalidad y adaptar su respuesta penal al ritmo del cambio tecnológico (Naranjo Hincapié, 2023).

En conclusión, el ordenamiento penal colombiano, aunque contempla la figura de la falsedad personal, no se encuentra actualmente preparado para enfrentar la complejidad que representa la suplantación de identidad mediante inteligencia artificial. Las normas vigentes no reconocen expresamente los contenidos sintéticos como medios comisivos ni ofrecen herramientas eficaces para sancionar delitos cometidos con tecnologías como los deepfakes. Esto genera vacíos jurídicos y debilita la respuesta del Estado frente a este fenómeno emergente.

Desde el enfoque criminológico, la suplantación algorítmica de identidad ha transformado radicalmente el perfil del delincuente y la dinámica de ejecución del delito, permitiendo acciones anónimas, transnacionales y automatizadas que vulneran la intimidad, la reputación y la seguridad de las personas. Resulta urgente y necesario adoptar un enfoque integral que combine reformas normativas, institucionales y preventivas para fortalecer la capacidad del sistema penal colombiano frente a estos nuevos desafíos. Esto incluye la creación de tipos penales específicos, el establecimiento de agravantes por uso de IA, la formación técnica de operadores judiciales, la implementación de tecnologías forenses especializadas y la promoción de la alfabetización digital ciudadana. Solo una articulación coherente entre ley, técnica y cultura permitirá enfrentar la suplantación algorítmica de identidad de forma efectiva y garantista.

Referencias

- Ámbito Jurídico. (2024). *Buscan crear el delito de suplantación de persona utilizando inteligencia artificial*. <https://www.ambitojuridico.com/noticias/noticias/penal/buscan-crear-el-delito-de-suplantacion-de-persona-utilizando-inteligencia>
- Centro de estudios regulatorios. (2022). *El derecho al control humano: una respuesta jurídica a la inteligencia artificial*. <https://www.cerlatam.com/publicaciones/el-derecho-al-control-humano-una-respuesta-juridica-a-la-inteligencia-artificial/>
- Corte Constitucional. (2024, agosto 2). *Sentencia T-323*, M.P Juan Carlos Cortés González. <https://www.corteconstitucional.gov.co/relatoria/2024/t-323-24.htm>
- Corte Suprema de Justicia, Sala Penal. (2020, febrero 5). *Sentencia 50853*, M.P José Francisco Acuña Vizcaya. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=91000&dt=S>
- Ley 599 de 2000. (2000, julio 24). *Por la cual se expide el Código Penal*. D.O No. 44.097. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388>
- Martínez, G. (2024). *Suplantación de identidad digital: hacia una necesaria tutela penal*. Revista de Derecho Público, 72(1). Universidad Internacional de la Rioja, España. <https://dialnet.unirioja.es/download/articulo/9598609.pdf>
- Ministerio de Justicia y del Derecho. (2019). *Suplantación de identidad en el proceso penal*. <https://www.minjusticia.gov.co/programas-co/LegalApp/Paginas/Que-puedo-hacer-si-tengo-antecedentes-penales-porque-suplantaron-mi-identidad-en-un-proceso-penal.aspx>

Naranjo Hincapié, S. (2023). *Suplantación de identidad: una mirada desde el derecho comparado*. <https://repository.ces.edu.co/server/api/core/bitstreams/02c1ce68-a9d8-4ff9-b7f0-8bfeed2ad314/content>

Regueiro, S. (2023). *El impacto de la inteligencia artificial en el ámbito legal*. Estudios Breves, (7). <https://dialnet.unirioja.es/descarga/articulo/9261251.pdf>

Sanabria, J. (2024). *La inteligencia artificial (IA) en fallos judiciales en Colombia: “Un juicio avanzado”*. Universidad Externado de Colombia.
<https://telecomunicaciones.uexternado.edu.co/la-inteligencia-artificial-ia-en-fallos-judiciales-en-colombia-un-juicio-avanzado/>

Santos, M. (2017). *Regulación legal de la robótica y la inteligencia artificial: retos del futuro*. Revista Jurídica de la Universidad de León, 25–50.

Superintendencia de Industria y Comercio. (2022). *Indebido tratamiento de datos personales por casos de suplantación de identidad*. <https://www.sic.gov.co/boletin/juridico/habeas-data/indebido-tratamiento-de-datos-personales-por-casos-de-suplantaci%C3%B3n-de-identidad>