# DESAFÍOS DE LA TIPICIDAD EN LA ERA DE LA INTELIGENCIA ARTIFICIAL: ANÁLISIS DE LA INSUFICIENCIA DEL RÉGIMEN PENAL COLOMBIANO

ALEJANDRA MARÍA BERNAL BOHORQUEZ



UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
MAESTRÍA EN DERECHO Y JUSTICIA
VILLAVICENCIO
2026

# DESAFÍOS DE LA TIPICIDAD EN LA ERA DE LA INTELIGENCIA ARTIFICIAL: ANÁLISIS DE LA INSUFICIENCIA DEL RÉGIMEN PENAL COLOMBIANO

ALEJANDRA MARÍA BERNAL BOHORQUEZ

Articulo académico presentado como requisito para optar por el título de Especialista en Derecho Penal y Sistema Penal Acusatorio

Asesor
Mg. RODRIGO CORTES BORRERO
Magister en Derecho contractual público y privado

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
MAESTRÍA EN DERECHO Y JUSTICIA
VILLAVICENCIO
2026

**Autoridades Académicas**

**P. Álvaro José ARANGO RESTREPO, O.P.**
Rector General

**P. Adrián Mauricio GARCÍA PEÑARANDA, O.P.**
Vicerrector Académico General

**P. Luis Antonio ALFONSO VARGAS, O.P.**
Rector Seccional Villavicencio

**P. Juan Francisco CORREA HIGUERA, O.P.**
Vicerrector Académico Seccional Villavicencio

**Mg. Julieth Andrea SIERRA TOBÓN**
Secretaria General Seccional Villavicencio

**Mg. Rodrigo CORTÉS BORRERO**
Decano Facultad de Derecho

## Dedicatoria

A mi más grande amor: mamá.
Por tu legado de nunca dejar de aprender.
Por enseñarme, con tu ejemplo, el valor de la justicia y la rectitud.
Por recordarme que debo vivir eligiendo aquello que llena mi alma y mi corazón.
Porque la vida es más bonita cuando se cree en uno mismo y se asume cada nuevo reto con preparación y valentía.
Esta meta también es tuya.
Gracias por ser mi raíz y mi impulso.
Y a Juan, el hombre que me ha enseñado que mis sueños son nuestros. Todo mi amor, hoy y siempre.

## Agradecimientos

La culminación del presente artículo de investigación representa no solo un logro académico, sino también el resultado del acompañamiento, la orientación y el apoyo de diversas personas e instituciones que hicieron posible este proceso, en especial al Dr. Rodrigo Cortes, asesor y mentor en el desarrollo de este sueño llamado maestría.

Agradezco a la institución universitaria por brindar los espacios académicos, recursos investigativos y escenarios de discusión que enriquecieron este trabajo. El acceso a bibliografía especializada y el intercambio de saberes con la comunidad académica fueron fundamentales para consolidar este estudio.

De manera especial, reconozco el apoyo de mi familia, cuya paciencia, comprensión y motivación constante fueron un pilar esencial durante este proceso. Su respaldo incondicional hizo posible dedicar el tiempo y la concentración necesarios para llevar a término esta investigación.

Finalmente, agradezco a todas aquellas personas que, de una u otra forma, aportaron ideas, comentarios o palabras de ánimo a lo largo de este camino académico. Cada contribución, por pequeña que pareciera, sumó al resultado final de este trabajo.

# Desafíos de la tipicidad en la era de la inteligencia artificial: análisis de la insuficiencia del régimen penal colombiano

***Alejandra María Bernal Bohorquez***

***Rodrigo Cortes Borrero (Dir)***

## Resumen

La presente investigación analiza los desafíos que la inteligencia artificial generativa, particularmente a través de tecnologías *deepfake*, plantea al principio de tipicidad en el derecho penal colombiano.

El presente trabajo de investigación analiza el marco normativo penal colombiano vigente partiendo de la ley 599 de 200, la reciente ley 2502 de 2025 y la ley 1273 de 2009, por medio de las cuales se responden de manera somera a la evolución tecnológica respecto del reconocimiento de la identidad digital sintética, dejando de igual manera vacíos normativos frente a las conductas como acoso digital, suplantación o manipulación mediante simulaciones audiovisuales.

Desde la perspectiva dogmática, el trabajo pone en evidencia una crisis del objeto material del delito y de las categorías clásicas de autoría y culpabilidad, especialmente cuando la conducta ilícita involucra sistemas autónomos o descentralizados de inteligencia artificial. La atribución de responsabilidad en escenarios de "autoría mediata por algoritmo" desafía las estructuras tradicionales del dolo y la imputación subjetiva. Asimismo, se identifican falencias procesales en materia probatoria, dado que el Ley 906 de 2004 no contempla protocolos específicos para la autenticación de contenidos sintéticos, lo que ralentiza la respuesta judicial y profundiza el daño reputacional de las víctimas.

En el ámbito jurisprudencial, se destaca el papel de la Corte Constitucional de Colombia, especialmente a través de la Sentencia T-280 de 2022, que reconoce el derecho a la imagen como un derecho fundamental autónomo y sienta bases para la protección de la identidad digital. No obstante, el estudio concluye que las decisiones de tutela, aunque relevantes, no sustituyen la necesidad de una reforma estructural del sistema penal.

Finalmente, el análisis de política criminal propone la creación de un tipo penal autónomo de usurpación de identidad sintética, la incorporación de la responsabilidad penal de personas

jurídicas en delitos de alta complejidad tecnológica, la implementación de mecanismos procesales ágiles como el "Habeas Data Criminal" y la adopción de sanciones restaurativas digitales orientadas a la desindexación y limpieza de huella digital. En suma, la investigación sostiene que el derecho penal colombiano enfrenta una insuficiencia estructural frente a los desafíos de la inteligencia artificial.

***Palabras clave*:** Deepkafe, Inteligencia Artificial, Derecho penal

## Abstract

This research analyzes the challenges that generative artificial intelligence, particularly through deepfake technologies, poses to the principle of legality in Colombian criminal law.

This research evaluates the adequacy of the current criminal law framework in Colombia, particularly since Law 599 of 2000 and the more recent Law 2502 of 2025, as well as its articulation with Law 1273 of 2009. It examines how the legislature has attempted to respond to technological sophistication by introducing aggravating circumstances and recognizing the notion of "synthetic digital identity," but also reveals regulatory gaps regarding conduct that does not pursue a direct economic objective, such as cyber harassment, online gender-based violence, or political manipulation through audiovisual simulations.

From a dogmatic perspective, the work highlights a crisis in the material object of crime and in the classical categories of authorship and culpability, especially when the illicit conduct involves autonomous or decentralized artificial intelligence systems. The attribution of responsibility in scenarios of "indirect perpetration by algorithm" challenges the traditional structures of intent and subjective imputation. Furthermore, procedural shortcomings in evidentiary matters are identified, given that Law 906 of 2004 does not include specific protocols for the authentication of synthetic content, which slows down the judicial response and exacerbates the reputational damage suffered by victims.

In the jurisprudential sphere, the role of the Constitutional Court of Colombia stands out, especially through Judgment T-280 of 2022, which recognizes the right to one's image as an autonomous fundamental right and establishes a foundation for the protection of digital identity. However, the study concludes that these protective orders, while relevant, do not replace the need for a structural reform of the criminal justice system.

Finally, the criminal policy analysis proposes the creation of an autonomous criminal offense of synthetic identity theft, the incorporation of criminal liability for legal entities in crimes of high technological complexity, the implementation of agile procedural mechanisms such as "Criminal Habeas Data," and the adoption of digital restorative sanctions aimed at de-indexing and digital footprint cleansing. In sum, the research argues that Colombian criminal law faces a structural deficiency in the face of the challenges of artificial intelligence, which requires a transformation.

***Keywords:*** Deepfake, Artificial Intelligence, Criminal Law

## Introducción

En un entorno digital cada vez más envolvente, los elementos visuales y sonoros predominan en nuestras interacciones. No obstante, esta presencia constante conlleva nuevas exposiciones a riesgos, siendo los deepfakes una de las más alarmantes. Estas creaciones, elaboradas con inteligencia artificial, constituyen una forma altamente avanzada de manipulación que puede distorsionar la percepción de la realidad, impactando tanto la vida de las personas como la confianza en el público. La habilidad de recrear rostros, voces y movimientos con una verosimilitud inquietante presenta un reto considerable para la verdad y la seguridad personal.

La tecnología detrás de los deepfakes ha evolucionado rápidamente, permitiendo que personas sin conocimientos técnicos avanzados puedan producir contenido falso convincente. Desde videos que muestran a figuras públicas diciendo o haciendo cosas que nunca ocurrieron, hasta la creación de material pornográfico no consentido o la suplantación de identidad para fraudes. Este fenómeno exige no solo una mayor alfabetización digital, sino también un marco legal robusto que proteja a los ciudadanos de sus posibles estragos.

Colombia, consciente del creciente riesgo que representan los contenidos generados por inteligencia artificial con fines maliciosos, ha clasificado los deepfakes dentro de su legislación como un delito. La alteración de la imagen o voz de una persona sin su consentimiento, especialmente si se utiliza para causar daño reputacional, económico o psicológico, es una infracción grave que atenta contra derechos fundamentales como la honra, el buen nombre, la privacidad y la identidad personal.

Aunque no existe una ley específica denominada «Ley Deepfake», las conductas asociadas a la creación y difusión de este tipo de material pueden encajar en diversas figuras penales ya existentes en el Código Penal colombiano. Estas incluyen delitos como la injuria y calumnia (cuando se busca desacreditar o atribuir falsamente un hecho delictivo), la violación de datos personales (si se utiliza información sensible sin permiso), la usurpación de identidad, la pornografía infantil (en casos extremos de manipulación de menores) o el fraude informático (cuando se busca un beneficio económico ilícito). La Fiscalía General de la Nación ha reiterado su compromiso en perseguir estas actividades ilícitas, subrayando la importancia de la denuncia ciudadana.

La ley 2502 de 2025 representa un gran avance en el desarrollo de la legislación penal colombiana y su adaptación a la nueva era del siglo XXI. Esta norma, la cual modifica el artículo 296 del código penal el cual refuerza las penas por falsedad personal por el uso de inteligencia artificial, lo cual simboliza una respuesta esencial como el inicio de la regulación de las nuevas tecnologías.

El aumento de las deepfakes y todas aquellas herramientas de suplantación digital han tenido como consecuencia la amenaza sin precedente de los objetos jurídicos como la identidad personal, la privacidad y veracidad de la información. Los casos de uso malicioso de estas herramientas han crecido de manera exponencial, desde la creación de contenido pornográfico no consensuado hasta la manipulación de procesos electorales y la comisión de fraudes financieros. En este contexto, la definición precisa que hace la ley del concepto de «DeepFake» como «la creación, modificación y utilización de un registro audiovisual mediante Inteligencia Artificial de manera que el registro parezca auténtico del discurso o conducta real de un individuo» demuestra una comprensión técnica adecuada del fenómeno. Esta claridad conceptual era indispensable para evitar vacíos normativos que pudieran ser explotados por quienes cometen estos delitos.

## Objetivos

### Objetivo general

Analizar el marco normativo penal colombiano en vigencia frente a las afectaciones producidas por medio de la Deepfake respecto del honor, identidad y dignidad humana con el fin

de establecer la necesidad de ajustes o producción legislativa que protejan la identidad digital.

**Objetivos específicos**

Describir el marco regulatorio penal actual aplicable a estas conductas, incluyendo los delitos de injuria y calumnia, así como los delitos informáticos previstos en la Ley 1273 de 2009.

Identificar los vacíos normativos, dogmáticos y procesales frente a los daños causados por contenidos sintéticos hiperrealistas, especialmente en materia probatoria y de determinación de autoría.

Realizar un análisis de política criminal que permita plantear alternativas de reforma legislativa, como la creación de un tipo penal autónomo o la ampliación de los delitos informáticos para incluir la suplantación identitaria mediante inteligencia artificial.

## Capítulo I:Marco regulatorio penal colombiano vigente frente a las afectaciones al honor, la identidad y la dignidad mediante tecnologías Deepfake.

La implementación de la inteligencia artificial generativa ha difuminado la realidad y la simulación en la cotidianidad. Una de las aplicaciones más controversiales de dicha tecnología es Deepfakes, los cuales son definidos como manipulaciones audiovisuales mediante algoritmos que logran suplantar, rostros, voces, comportamientos de manera muy realista. En el contexto normativo colombiano dicho avance tecnológico también representa una amenaza directa a derechos fundamentales consagrados en la carta magna como el honor, el buen nombre y la dignidad humana.

No es de desconocimiento para los juristas que el Código Penal colombiano en ocasión a su antigüedad carece de herramientas para abordar las consecuencias jurídicas que conllevan el desarrollo tecnológico y la aplicación de la inteligencia artificial, no obstante los recurrentes casos de pornografia no consentida y fraudes por suplantación de identidad, ha generado la necesidad latente al Estado colombiano de generar un marco regulatorio más robusto con el fin de proteger dichos objetos jurídicos. La Ley 2502 de 2025 actualiza la punibilidad respecto de los riesgos de identidad digital.

El incontrolable avance de la inteligencia artificial en nuestra cotidianidad ha creado desafíos sin precedentes en el ámbito jurídico no solo en Colombia sino también de manera global. Una de sus manifestaciones más abruptas y peligrosas es los deepfakes, que desde una perspectiva de entretenimiento es algo inofensivo, pero al evaluar de fondo su composición ha de entenderse que puede ser muy peligroso ya que son contenidos audiovisuales generados mediante algoritmos de aprendizaje que permiten suplantar la imagen, voz y gesto de cualquier persona con una nivel de realismo ato y por lo tanto pueden hacer caer en error la percepción humana. Este fenómeno ha dejado de ser una innovación tecnológica para convertirse en una herramienta de vulneración de derechos fundamentales lo cual ha tenido como consecuencia que el Estado colombiano debe implementar en su ordenamiento jurídico, penas que castiguen dicho uso de estas herramientas. La problemática central que surge de la aplicación de dichas tecnologías radica en la tensión por la creación libre de contenido tecnológico y la protección de bienes jurídicos tutelados como el honor, identidad y dignidad humana, los cuales se encuentran contemplado en la ley 2503 de 2025 como herramienta legislativa de defensa respecto de dicha disyuntiva.

Para realizar un análisis profundo respecto de la regulación normativa vigente y la necesidad de la misma, ha de entenderse que dicho fenómeno tecnológico opera sobre la base de Redes Generativas Antagónicas, las cuales tienen como objeto el procesamiento de datos biométricos para crear presentaciones sintéticas. Diciendo de una manera más sencilla por medio del análisis de las facciones de una persona se pueden crear imágenes o videos replicándose haciendo cualquier acción que disponga la persona con dicha tecnología.

Ahora bien, desde un análisis jurídico de lo anterior ha de entenderse que la capacidad de alteración de la realidad invade las aristas del derecho a la propia imagen del cual la Corte Constitucional en sentencia T-280-2022 ha establecido un derecho autónomo e inalienable de las personas. Antes de la reforma del Código Penal con la ley 2502 de 2025 dichos delitos ocasionados por medio de estas herramientas tecnológicas eran castigados de manera habitual por medio de punibles clásicos como falsedad personal o injuria. No obstante el continuo avance de la inteligencia artificial ha dejado ver la existencia de un vacío normativo respecto de los métodos tradiciones de probanza y los verbos rectores que los delitos ya existentes no abarcan la realidad de la suplantación digital automatizada.

El uso de estas herramientas para crear, por ejemplo, pornografía no consentida o declaraciones falsas hiperrealistas, es considerado ahora una "vía de hecho" digital. La

jurisprudencia de la Sala de Casación Penal de la Corte Suprema de Justicia ha comenzado a integrar estos conceptos, señalando que la deshonra producida por medios tecnológicos tiene un efecto expansivo y permanente en la red, lo que justifica una tutela penal más agresiva. En el marco regulatorio de la actualidad se establece que la Fiscalía General de la Nación ha de tener las unidades especializada para certificar la autenticidad del material, así garantiza que el debido proceso se mantenga inocuo frente a la dificultad de distinguir lo real de o artificial.

Ha de resaltarse de igual manera que por medio del bloque de constitucionalidad y las directrices contempladas por la Universidad Externado de Colombia (2021), se sugiere que la protección de la identidad frente a la implementación de la inteligencia artificial ha de ser integral no solo desde la prevención sino también desde la responsabilidad penal y civil. En consecuencia a ello en la actualidad se desarrolla un proyecto de ley 043 de 2025 el cual contempla la implementación del código penal colombiano mediante la obligación de etiquetar que contenido es creado por medio de inteligencia artificial con el fin de diferenciarlo por parte de las autoridades y asi evitar la afectaciones a bienes jurídicos como el honor.

En conclusión, el marco regulatorio penal colombiano frente a los deepfakes ha evolucionado desde una interpretación analógica de normas antiguas hacia un sistema especializado que reconoce la peligrosidad de la IA generativa. La Ley 2502 de 2025 se erige como la piedra angular de esta defensa, tipificando y agravando las conductas que vulneran la identidad y el honor mediante simulaciones tecnológicas. Sin embargo, el desafío para el Estado colombiano en los próximos años será la implementación técnica de estas normas y la cooperación internacional, dado que la tecnología deepfake ignora las fronteras nacionales. La protección de la dignidad humana en la era de la IA requiere no solo de leyes robustas, sino de un sistema judicial capaz de entender y procesar la evidencia digital con la misma velocidad con la que los algoritmos crean nuevas realidades

## Capítulo II: Vacíos normativos, dogmáticos y procesales para la tutela judicial efectiva de las víctimas de suplantación identitaria sintética

El concepto de tutela judicial efectiva, consagrado en el artículo 29 de la Constitución Política de Colombia y reforzado por el Sistema Interamericano de Derechos Humanos, supone no sólo el acceso a la administración de justicia, sino la obtención de una respuesta pronta, fundada

en derecho y capaz de restaurar el bien jurídico vulnerado. No obstante, frente a la suplantación de identidad sintética nuestro ordenamiento jurídico posee falencias de gran relevancia que impiden la protección de los bienes jurídicos de manera integral. Los esfuerzos legislativos recientes son insuficientes tales como la ley 2501 de 2025 la cual posee vacíos en la normatividad que la configura respecto de la construcción dogmática del tipo penal y la operatividad de protocolos procesales, por lo cual esto tiene como resultado la desprotección de las víctimas cuya identidad es flagelada o alterada por la inteligencia artificial.

## I. El vacío normativo: La insuficiencia de la Ley 2502 frente a la ubicuidad digital

El primer obstáculo para la tutela efectiva reside en la naturaleza reactiva de la ley. La Ley 2502 de 2025, si bien introdujo agravantes para la suplantación mediante IA, se centró primordialmente en la falsedad personal y el fraude bancario. El vacío normativo surge cuando la suplantación no persigue un fin económico claro, sino una afectación existencial o política. En nuestro ámbito penal actual, la tipicidad es confusa cuando en la configuración de una conducta punible se aplican los deepfakes, en tales como el acoso, la injuria o la violencia de genero que no se puede establecer dentro de os tipo penales como pornografia infalnti o injuria tradicional en ocasión los elementos del tipo. Como sostiene la Universidad Externado de Colombia (2021), nuestro sistema legislativo aún no tiene la capacidad de reconocer la identidad sintética como un objeto jurídico de protección de manera autónoma, lo que tiende a obligar a los operadores judiciales a realizar maniobras interpretativas de la norma para poder ajustar dichos delitos diseñados para ámbitos de aplicación tradicional y no tecnológicos.

Adicional a lo anterior, existe un vacío normativo respecto de la regulación de la responsabilidad de los intermediarios tecnológicos, esto quiere decir de las plataformas que se utilizan para la afectación de estos bienes jurídicos. La Unión Europea por medio del Reglamento de la inteligencia Artificial establece diferentes obligaciones respecto de la transparencia de las plataformas que alojan contenido sintéticos, por lo cual dicha jurisdicción es un ejemplo de la implementación de esta problemática a la cual Colombia ha guardado silencio hasta el momento respecto de la responsabilidad solidaria de las redes sociales en la mitigación del daño. Dicha omisión en nuestra normativa impide que las víctimas de manera cautelar soliciten la eliminación de dicho contenido por medio de mandato judicial y choca con la extraterritorialidad de las empresas tecnológicas.

## II. Vacíos dogmáticos: La crisis del objeto material y la culpabilidad

Desde la dogmática penal, la suplantación identitaria sintética pone en crisis conceptos fundamentales. El primero es el objeto material del delito. En la suplantación tradicional, se usurpa la identidad de un sujeto vivo para suplantar su voluntad; en el deepfake, se crea una "persona digital" que dice y hace cosas que el original jamás haría. El vacío dogmático aquí es la falta de una teoría del daño a la "verdad personal". La dogmática tradicional castiga las lesiones al patrimonio pero aun no castiga la alteración de la realidad perceptiva, esto quiere decir que si por medio de un deepfake se visualiza un político recibiendo un soborno, l bien jurídico afectado es la integridad moral, mas no de por si, la alteración de la realidad y las consecuencias del mismo, por lo tanto, dicha imagen crea una carga de la prueba a la defensa ya que esta ha de probar que no es ella defendiendo de por sí su propia existencia teniendo o no los recursos para hacerlo.

De igual manera, otro vacío es evidente en la atribución de la culpabilidad y la autoría, esto radica en que la inteligencia artificial no funciona por sí sola y para la generación de estos deepfakes se debe relacionar un recurso humano, por lo tanto, la responsabilidad generada para dicho sujeto por la producción de las imagenes aun no siendo dicho persona la que los utilice para la implementación de una configuración de una conducta punible, ya que estaríamos hablando de un título de imputación nuevo tal como la autoría mediata por algoritmo.

La falta de una construcción dogmática sobre la responsabilidad por el producto y la autoría en entornos descentralizados deja a la víctima en un laberinto de imputaciones fallidas, donde el fiscal no logra individualizar al responsable bajo los estándares del dolo tradicional.

## III. Falencias procesales y el reto de la evidencia digital forense

En el plano procesal, la tutela judicial efectiva se desvanece ante la obsolescencia de los medios de prueba. El Código de Procedimiento Penal (Ley 906 de 2004) no posee protocolos para la identificación o autenticación de contenido sintético. Uno de los vacíos procesales más relevantes que se puede evidenciar en torno a esta problemática es la ausencia de una presunción de sospecha sobre el contenido digital, esto quiere decir que en casos que se denuncie por suplantación, ha de sospecharse en primer lugar la veracidad del contenido ya que, actualmente es la víctima la que posee la carga probatoria de peritajes privados para demostrar que un video es un

deepfake ya que la Fiscalía no posee las herramientas y no toma con seriedad el caso.

Un aspecto de gran importancia es que los laboratorios de criminalistica en Colombia son insuficientes para la demanda actual que se posee, ahora bien, con la implementación de dichos delitos información y las herramientas tecnológicas que han convertido aún más extenuante dicho trabajo, el peritaje de que determine la autenticidad de un video mediante análisis de ruido inconsistencias biométricas puede tardar mucho tiempo, tiempo que daña la dignidad y el honor de la víctima de manera irreversible.

La víctima se encuentra ante una justicia que camina a paso de papel mientras la agresión viaja a la velocidad de la fibra óptica.

## IV. Hacia una Tutela Judicial Efectiva: Jurisprudencia y Retos

La Corte Constitucional, en sentencias como la T-280 de 2022 y la SU-420 de 2019, ha intentado cerrar estos vacíos mediante la interpretación de los derechos fundamentales. La Corte ha enfatizado que, en el entorno digital, el juez debe actuar como un protector proactivo. De igual manera, ha de tenerse en cuenta que dichas providencias poseen únicamente un efecto inter partes, esto quiere decir que no solucionan el problema estructural del sistema penal.

La tutela efectiva exige que el proceso penal sea capaz de restaurar el "derecho a la verdad". En los casos de suplantación sintética, la reparación no debería ser solo pecuniaria, sino técnica: la obligación de publicar la sentencia de inautenticidad con metadatos que impidan su futura viralización. La ausencia de este tipo de sanciones restaurativas en el Código Penal colombiano demuestra que el sistema aún concibe el delito como un suceso estático y no como un fenómeno digital dinámico.

Es claro que el marco normativo actual ha tenido un avance significativo comparado con el de la última década, aunque también ha de tenerse en cuenta que su desarrollo respecto de la dogmática y la materia procesal frente a este tema ha sido mínimo. Los vacíos normativos referentes a la responsabilidad de plataformas, la rigidez de la teoría del delito y las barreras procesales respecto de los procesos probatorios forenses son barreras respecto del acceso a la justicia.

## Capítulo III: Análisis de política criminal y propuestas de reforma legislativa para la protección penal de la identidad digital frente a la inteligencia artificial.

En conclusión, el marco regulatorio penal colombiano frente a los deepfakes ha evolucionado desde una interpretación analógica de normas antiguas hacia un sistema especializado que reconoce la peligrosidad de la IA generativa. La Ley 2502 de 2025 se erige como la piedra angular de esta defensa, tipificando y agravando las conductas que vulneran la identidad y el honor mediante simulaciones tecnológicas. Sin embargo, el desafío para el Estado colombiano en los próximos años será la implementación técnica de estas normas y la cooperación internacional, dado que la tecnología deepfake ignora las fronteras nacionales. La protección de la dignidad humana en la era de la IA requiere no solo de leyes robustas, sino de un sistema judicial capaz de entender y procesar la evidencia digital con la misma velocidad con la que los algoritmos crean nuevas realidades.

### I. Diagnóstico de la Política Criminal Actual y el Populismo Punitivo Digital

El primer eje de análisis revela que la política criminal colombiana en materia de IA ha caído parcialmente en lo que la doctrina denomina "populismo punitivo digital". La respuesta legislativa inmediata a los escándalos de *deepfakes* pornográficos o fraudes biométricos ha sido el incremento de penas, bajo la premisa errónea de que la gravedad de la sanción disuadirá a ciberdelincuentes que operan desde el anonimato y la extraterritorialidad. Esta perspectiva no contempla que en el ámbito de la inteligencia artificial generativa, la eficiencia del derecho penal no recaiga sobre la imposición de la pena sino en la posibilidad de capturas y en la capacidad de atribuir responsabilidad penal.

La política criminal implementada hoy en dia no posee una estrategia de vinculación de empresas tecnológicas con el fin de cooperar y así poseer los recursos necesarios para la protección de la identidad digital supeditada a denuncias individuales que simplemente se estancan en la fase de indagación preliminar por falta de realización de peritajes técnicos especializados en esta área.

Como señala Morrón Bonnett (2025), una política criminal coherente debe transitar del castigo del resultado a la regulación del riesgo. En Colombia, la carencia de normativa penal que tenga como finalidad sancionar únicamente la creación malintencionada de herramientas de

suplantación como un tipo penal de conducta y no de fin, sin importar si se causa o no un daño patrimonial o personal, representa un vacío de protección y prevención a la identidad digital . Por tanto, la política criminal debe evolucionar hacia una "criminalización de las conductas preparatorias" de alta peligrosidad tecnológica, siempre respetando el principio de lesividad.

## II. Propuesta de Reforma Legislativa: La Creación del Tipo Penal de Usurpación de Identidad Sintética

Ante la insuficiencia de los artículos 220 (injuria) y 296 (falsedad personal) del Código Penal, se propone una reforma estructural que introduzca el tipo penal autónomo de "Usurpación de la Identidad Sintética mediante Sistemas de Inteligencia Artificial". Dicha propuesta de un delito autónomo respecto de la protección de la identidad digital no ha de contener únicamente el verbo rector de suplantar sino de igual manera el generar, difundir o comercializar dichas representaciones sintéticas con el fin de prevenir dichas conductas con el fin de no menoscabar la dignidad, honor o autonomía.

Dicha reforma ha de incluir además una responsabilidad penal de las personas jurídicas en delitos informáticos en ocasión a su rol de intermediarios en la creación de dicho contenido, aunque ha de tenerse en cuenta que en Colombia aún no existe la responsabilidad penal para personas jurídicas sino únicamente responsabilidad civil, de igual manera la responsabilidad penal es individual, lo que ha de establecer que las empresas de software que operan con negligencia grave respecto de la regulación del uso de dichos algoritmos quedan impunes.

## III. Reforma Procesal y el "Habeas Data Criminal"

En el plano procesal, la propuesta se encamina hacia la creación del "Habeas Data Criminal". Este mecanismo permitiría que cualquier ciudadano, ante la sospecha razonable de estar siendo víctima de una suplantación sintética, pueda solicitar ante un Juez de Control de Garantías la suspensión inmediata de la difusión de dicho contenido en plataformas digitales, sin necesidad de agotar la vía administrativa de la red social. La política criminal debe dotar al juez penal de facultades para emitir órdenes de "congelación de evidencia digital" en tiempo real.

La reforma del Código de Procedimiento Penal ha de incluir de igual manera la presunción

de licitud del contenido sintético que no se encuentre etiquetado, por lo tanto si un contenido que afecta la honra de un tercero que ha sido generado por inteligencia artificial y que no se encuentra etiquetado se ha de entender de dicha providencia y puede solicitarse de manera cautelar su sustracción con el fin de proteger a la víctima de dicha conducta delictiva. Esto invierte la carga de la diligencia: las plataformas y los creadores tendrán la obligación de demostrar la transparencia de sus procesos para evitar la intervención penal.

## IV. Hacia una Justicia Restaurativa Digital

Finalmente, el análisis de política criminal debe contemplar la reparación. En los delitos de identidad digital, la cárcel es a menudo una respuesta insuficiente para la víctima, cuya imagen sigue circulando en la red. Se propone la creación de la "Sanción de Restauración Digital", que obligue al sentenciado y, subsidiariamente, a la plataforma mediadora, a realizar procesos de limpieza de huella digital y desindexación de los contenidos fraudulentos. La verdadera justicia para una víctima de *deepfake* no es solo ver al infractor sancionado, sino recuperar el control sobre su propia representación en el ciberespacio. Como sugiere la Universidad Externado de Colombia (2021), la reparación en la era de la IA debe ser técnica y no puramente simbólica.

La protección de la identidad frente al desarrollo de la inteligencia artificial en nuestro ordenamiento jurídico requiere de un giro de gran relevancia en su política criminal no solo enfocado en la criminalización de la innovación tecnológico sino la protección del yo digital que hoy en día toma gran relevancia al igual que el cuerpo físicos, por lo cual las reformas propuestas con anterioridad constituyen una ruta de inicio para que el derecho penal colombiano deje de ser un espectador pasivo respecto del avance tecnológico y tome un rol activo y de ejemplo en la comunidad latinoamericana . La tutela judicial efectiva sólo será posible cuando el Estado entienda que, en el siglo XXI, la suplantación de la realidad es la más grave de las falsedades.

## Conclusiones

El fenómeno de la inteligencia artificial generativa y, en particular, la proliferación de tecnologías *deepfake*, ha puesto en evidencia que el derecho penal colombiano opera aún bajo categorías diseñadas para un entorno analógico. Aunque la expedición de la Ley 2502 de 2025

representa un avance significativo al reconocer la gravedad de la suplantación identitaria mediante IA, su enfoque sigue siendo predominantemente reactivo y centrado en el aumento de penas, sin resolver de manera estructural los problemas de tipicidad y atribución de responsabilidad.

En el plano normativo, persiste una insuficiente protección de la identidad digital como bien jurídico autónomo. La regulación actual obliga a encuadrar las conductas de suplantación sintética dentro de tipos penales tradicionales como la injuria, la calumnia o la falsedad personal, lo que genera interpretaciones extensivas que pueden tensionar el principio de legalidad. Esta situación revela la necesidad de un tipo penal específico que reconozca la identidad digital como una dimensión esencial de la personalidad humana en el siglo XXI.

Desde la dogmática penal, la irrupción de sistemas algorítmicos plantea una crisis en las categorías clásicas de autoría, culpabilidad y objeto material del delito. La figura del autor mediato por medio de un algoritmo, la posible concurrencia de responsabilidades entre programadores, usuarios y plataformas, y la autonomía operativa de ciertos sistemas de IA exigen una reconstrucción teórica que permita mantener la coherencia del sistema penal sin sacrificar garantías fundamentales.

En el ámbito procesal, la lentitud en la práctica de pruebas forenses digitales y la ausencia de mecanismos cautelares ágiles agravan el daño sufrido por las víctimas. La justicia penal no puede responder con procedimientos tradicionales a agresiones que se expanden con la inmediatez de la red. Por ello, resulta indispensable modernizar el Ley 906 de 2004 e incorporar protocolos específicos para la autenticación de contenido sintético, así como medidas urgentes de suspensión y desindexación.

En términos de política criminal, el Estado colombiano debe abandonar el populismo punitivo digital y adoptar una estrategia integral que combine prevención tecnológica, cooperación internacional, responsabilidad empresarial y justicia restaurativa. La protección efectiva de la dignidad humana en entornos digitales no depende exclusivamente del aumento de penas, sino de la capacidad institucional para identificar, rastrear y neutralizar rápidamente las afectaciones a la identidad.

En definitiva, la investigación demuestra que la insuficiencia del régimen penal colombiano frente a la inteligencia artificial no es únicamente normativa, sino estructural. La era digital exige un replanteamiento profundo del principio de tipicidad, de los bienes jurídicos protegidos y de los mecanismos procesales, con el fin de garantizar que la identidad digital reciba

el mismo nivel de tutela que la identidad física. Solo a través de una reforma coherente, técnica y garantista será posible asegurar una verdadera tutela judicial efectiva en un contexto donde la simulación algorítmica amenaza con redefinir los límites de la verdad y la responsabilidad penal.

## Referencias

Congreso de la República de Colombia. (28 de julio de 2025). Ley 2502 de 2025. *Por medio de la cual se modifica y establece un agravante al artículo 296 de la Ley 599 del 2000, Código Penal Colombiano y se dictan otras disposiciones*. Diario Oficial No. 53198. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=188454

Corte Constitucional de Colombia. (3 de febrero de 2017). Sentencia T-060. *Magistrado Ponente: Gabriel Eduardo Mendoza Martelo*. https://www.corteconstitucional.gov.co/relatoria/2017/t-060-17.htm

Corte Constitucional de Colombia. (12 de septiembre de 2019). Sentencia SU-420. *Magistrado Ponente: Jospe Fernando Reyes Cuartas*. https://www.corteconstitucional.gov.co/relatoria/2019/su420-19.htm

Corte Constitucional de Colombia. (8 de agosto de 2022). Sentencia T-280. *Magistrado sustanciador: José Fernando Reyes Cuartas*. https://www.corteconstitucional.gov.co/relatoria/2022/t-280-22.htm

Fiscalía General de la Nación. (2025). Manual de procedimiento para la recolección y análisis de evidencia digital en delitos cometidos mediante Inteligencia Artificial. Imprenta Nacional de Colombia.

Fiscalía General de la Nación. (2025). Retos de la evidencia digital en la persecución de delitos informáticos. Fiscalía General de la Nación.

Gil Domínguez, A. (2019). *Inteligencia artificial y Derecho.* Rubinzal Culzoni.

Morales Neira, M. L. (2021). Uso y divulgación de la imagen personal e interacción con la Inteligencia Artificial. *Revista La Propiedad Inmaterial*(30), 169-197. https://doi.org/10.18601/16571959.n30.07.

Morrón Bonnett, E. J. (2025). La pornografía "deepfake": retos legales y necesidad de intervención. *Nuevo Foro Penal, 21*(104), 82-115. https://dialnet.unirioja.es/descarga/articulo/10263803.pdf

Peláez Ortiz, F. J. (7 de noviembre de 2025). Delito, algoritmo y responsabilidad: el Derecho Penal ante la era digital. *Penaltech Insignts*. https://www.linkedin.com/pulse/delito-algoritmo-y-responsabilidad-el-derecho-penal-la-pel%C3%A1ez-ortiz-biynf/?originalSubdomain=es

Savvia Legal. (21 de agosto de 2025). *Deepfakes y derecho penal: el desafío regulatorio que enfrenta Colombia con la expedición de la Ley 2502 de 2025*. https://savvialegal.com/2025/08/21/deepfakes-y-derecho-penal-el-desafio-regulatorio-que-enfrenta-colombia-con-la-expedicion-de-la-ley-2502-de-2025/

Senado de la República de Colombia. (7 de mayo de 2025). Proyecto de Ley No. 043 de 2025: Regulación ética de la Inteligencia Artificial en Colombia. Ministerio de Ciencia, Tecnología e Innovación. https://minciencias.gov.co/sites/default/files/upload/noticias/pl_ia_finalizado.pdf

Unesco. (2021). *El aporte de la inteligencia artificial y las TIC avanzadas a las sociedades del conocimiento: una perspectiva de derechos, apertura, acceso y múltiples actores.* Ediciones Unesco. https://unesdoc.unesco.org/ark:/48223/pf0000375796