

Intervención del Estado colombiano frente al uso ilícito de inteligencia artificial y su impacto en el derecho humano a la propia imagen. Análisis comparado entre Colombia y Brasil¹

Bridgeth Yorlady Pérez Lizarazo²

Yesica Alejandra Pérez Pereira³

Jairo Odair Ruiz Piñeros⁴

Juan Pablo Moncada Flórez / Director⁵

Resumen

El presente artículo de reflexión realiza un estudio del marco normativo y jurisprudencial del derecho humano a la propia imagen y la protección de la identidad personal en Colombia y Brasil. La presente investigación adopta un enfoque cualitativo, documental y dogmático-jurídico, complementado con un método comparado aplicado a los ordenamientos de Colombia y Brasil. Derechos que en la actualidad se ven amenazados por el uso malicioso o ilícito de la inteligencia artificial (IA). , Una de las modalidades de ese uso ilícito de la IA d es la falsedad personal por medio de las llamadas *deepfakes* y *deepfakes* sexuales. Estas modalidades afectan especialmente a mujeres y niñas, en calidad de víctimas, configurándose como otra modalidad de violencia de género por medio del uso de nuevas tecnologías. Se describe el uso ilícito de la IA, se enumeran las principales modalidades de esta y se ofrece una mirada al impacto de dicha tecnología en la comisión de conductas punibles en Colombia y Brasil. Asimismo, se analiza la intervención normativa que ambos estados adoptan para proteger el derecho a la propia imagen ante el uso ilícito de la IA. También se observa un estudio sobre el estado de la regulación normativa en relación con los *deepfakes* sexuales en Colombia y Brasil. Con el panorama más claro, se lograron realizar propuestas para subsanar los vacíos legales existentes, como implementar las circunstancias de mayor punibilidad en la comisión de conductas punibles en general y en la falsedad personal cometida empleando la IA. Finalmente, se logra concluir que tanto Colombia como Brasil presentan vacíos normativos y que, en la actualidad, pese a existir proyectos de ley

¹ Artículo científico presentado como opción de grado para optar por el título de Magíster en derecho

² Abogada egresada de la Universidad Industrial de Santander UIS. Abogada litigante independiente en derecho penal y derecho de familia. Maestrante de la Universidad Santo Tomás de Bucaramanga. Correo Electrónico: abogadabridgethperez@gmail.com

³ Abogada egresada de la Universidad de Cartagena en el año 2013, especialista en Derecho Penal en el año 2016 y Ciencias Criminológicas de la Universidad de Cartagena, y Derecho Procesal por la Universidad Santo Tomás, en el año 2018. Funcionaria de la Rama Judicial, actualmente en el cargo de Juez Promiscuo Municipal de Santa Bárbara, Santander. Correo Electrónico: Jeal_pepe@hotmail.com

⁴ Abogado egresado de la Universidad Católica de Colombia en el año 2008, especialista en Derecho Penal en el año 2014 por la Universidad Autónoma de Bucaramanga, especialista en Derecho Constitucional en el año 2018 por la Universidad Nacional de Colombia. Correo electrónico jaiorupi@yahoo.com

⁵ Abogado, Universidad Santo Tomás, Bucaramanga, Magíster en Derecho de las Nuevas Tecnologías, Universidad de Granada, España. Doctor, Universidad de Granada, España. Investigador Senior/ Consultor Privacidad Transformación Digital/ ODP/ Docente Conferencista/ Socio Legal Shield. Correo electrónico juan.moncada@legalshield.com.co - juan.moncada@ustabuca.edu.co

bienintencionados, cualquier penalización de estos fenómenos se debe hacer con delitos preexistentes.

Palabras clave: Inteligencia Artificial Deepfake, Violencia de Género, Delito, Colombia, uso ilícito, Brasil.

Intervention of the Colombian State in the Face of the Illicit Use of Artificial Intelligence and its Impact on the Human Right to One's Own Image: A Comparative Analysis Between Colombia and Brazil.

Abstract

This reflective article studies the legal and jurisprudential framework of the human right to one's own image and the protection of personal identity in Colombia and Brazil. These rights are currently threatened by the malicious or illicit use of artificial intelligence (AI). It emphasizes that these threats have increased significantly in these two societies, especially the falsification of personal identity through so-called *deepfakes* and sexual *deepfakes*. These methods disproportionately affect women and girls as victims, establishing themselves as another form of gender-based violence perpetrated through the use of new technologies. The article describes the illicit use of AI, outlines its main forms, and examines the impact of this technology on the commission of criminal offenses in Colombia and Brazil. It also analyzes the legal interventions in both countries regarding the protection of the right to one's own image against the illicit use of AI. Finally, it examines the state of regulations concerning sexual *deepfakes* in Colombia and Brazil. With a clearer picture, proposals were made to address existing legal gaps, such as implementing aggravated penalties for criminal conduct in general and for identity theft committed using AI. Ultimately, it was concluded that both Colombia and Brazil have regulatory gaps and that currently, despite well-intentioned bills, any criminalization of these phenomena must be based on pre-existing offenses.

Keywords: Artificial Intelligence, Deepfake, Gender Violence, crime, Colombia, illicit use, Brazil.

Introducción

Los Estados colombiano y brasileño en la actualidad enfrentan como reto la proliferación y transversalidad de los sistemas de inteligencia artificial en los entornos virtuales. Esto se ha generalizado en todas las áreas digitales; esto incide en la afectación de los derechos humanos debido a que se está generando una nueva era digital artificial en la que el concepto de realidad se ve permeado y difícil de afirmar.

Debido a esta afectación, el mundo digital permanece en peligro y genera que la humanidad sea potencialmente víctima de un engaño difícil de controlar, porque la imagen de las personas se afecta por una serie de ataques interminables, que evolucionan rápidamente con el uso indiscriminado de la Inteligencia Artificial y los esfuerzos por combatirlos se ven rezagados con el solo paso del tiempo, en la medida que el actuar humano no logra anticipar con facilidad las

nuevas modalidades de uso indebido de la tecnología y por ello no se puede proteger con facilidad la propia imagen.

Las acciones institucionales en regulación desplegadas por Colombia y Brasil ante el avance y uso de la de la inteligencia Artificial mediante políticas públicas, ejemplo de ello es que, Brasil por su parte tiene una regulación en estos aspectos y Colombia tiene contemplada en su legislación penal, situaciones que agravan las penas por el uso indiscriminado de la inteligencia artificial, siguiendo más rápido con proyectos de ley y jurisprudencia constitucional sobre el tema de *deepfakes* (que son contenidos audiovisuales, como videos, imágenes o audios, creados o manipulados mediante inteligencia artificial, cuyo objetivo primordial es hacer creer que una persona es real al ser humano, y da a entender que ha dicho, mencionado o hizo algo que en realidad no ocurrió, este término *deepfakes*, falso, da una apariencia de verdad en algo que no lo es). (Fortinet, 2026)

En el año 2019, Colombia publicó en su Política Pública de transformación digital e inteligencia artificial (CONPES) los lineamientos fijados por la OCDE y fijó cuatro objetivos específicos, así como 14 líneas de acción, que incluyen la creación de un mercado de inteligencia artificial ética para su desarrollo e implementación (Consejo Nacional de Política Económica y Social, 2019).

En el año 2022, con el Decreto 767, Colombia también implementó una política llamada Gobierno Digital; en este documento se mostraron principios y herramientas tanto para el sector público como para el privado que fortalecen una implementación responsable de la inteligencia artificial y los nuevos desafíos (Presidencia de la República de Colombia, 2022).

Por su parte, Brasil tiene la Ley General de Protección de Datos (LGPD), que regula y hace una innovación tecnológica con garantías constitucionales de privacidad, dignidad, igualdad y no discriminación, buscando abordar los riesgos de sesgo, vigilancia, manipulación informativa y decisiones automatizadas que afectan derechos fundamentales (Presidencia de la República Federativa de Brasil, 2018).

Ante tal escenario, donde el uso de la tecnología avanzada la Inteligencia Artificial desafía a todos los Estados incluido el colombiano y el de Brasil, en cuanto a la protección de los derechos humanos de las personas, se evidencia la necesidad de verificar y contrastar las regulaciones normativas de temas como el uso indebido de datos personales, y de ahí es que surge la necesidad de estudiar a profundidad la naturaleza, alcance y desafíos que el uso ilícito de la IA en países latinoamericanos como Colombia y Brasil.

Por lo anterior, el presente artículo se propone como objetivo principal analizar desde la perspectiva jurídico-penal la respuesta del ordenamiento jurídico colombiano frente a la protección del derecho fundamental a la propia imagen de cara al uso ilícito de la IA para la comisión de conductas punibles.

Para ello, se partirá por **1.)** analizar el derecho humano a la propia imagen y su relación con la protección de la identidad personal, seguidamente **2.)** se estudiará el impacto de la Inteligencia artificial en la comisión de conductas punibles, realizando una comparación entre

Colombia y Brasil, así mismo, **3.)** se explicará las similitudes y diferencias del Estado de Brasil y Colombia en cuanto a la forma de intervención frente a la protección del derecho humano a la propia imagen y finalmente, **4.)** se propondrá posibles formas de intervención del Estado colombiano que brinden garantías de protección de la propia imagen atendiendo a principios de legalidad, proporcionalidad y necesidad de la intervención penal, revisando la experiencia brasileña que al respecto existe.

1. Derecho humano a la propia imagen y su relación con la protección de la identidad personal

Como punto de partida, se debe conceptualizar el derecho humano a la propia imagen, toda vez que dicho objeto constituirá el eje del análisis comparativo respecto a las acciones de salvaguarda implementadas por Colombia y Brasil para su protección, y para ello, se estudiará cómo se ha entendido en los dos marcos normativos, en la medida en que su conceptualización no ha sido exactamente igual.

1.1. Derecho humano a la propia imagen en Colombia

En Colombia, la propia imagen no se encuentra expresamente contemplada en la Constitución Política como un derecho; sin embargo, como quiera que la propia imagen es un dato personal, su protección se enmarca tácitamente dentro del derecho fundamental al reconocimiento del estatus de persona jurídica y al hábeas data, contemplados en los arts. 14 y 15, precisando en la última disposición, entre sus componentes que “En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución” (Asamblea Nacional Constituyente, 1991).

De ahí que se pueda afirmar que el desarrollo legislativo de protección del derecho a la propia imagen se encuentra en el reglamento del derecho a la protección de datos personales, expedido por el legislador colombiano en la Ley Estatutaria 1581 de 2012.

Esta ley estatutaria establece que todas las personas tienen el derecho a conocer, actualizar y rectificar las informaciones que se hubiesen recaudado en bases de datos o archivos de ellas, y establece una categoría restringida de datos sensibles vinculados a la esfera íntima con potencial discriminatorio (Congreso de la República de Colombia, 2012), por ello, se constituye en la norma más importante para tal efecto, pues establece que la imagen (fotos, videos, datos biométricos) es un dato personal, el uso de la imagen permite la identificación biométrica automatizada, y se puede clasificar como un dato sensible, respecto del cual se requiere autorización previa, expresa e informada del titular para su captura, almacenamiento o difusión.

Ahora, no ocurre lo mismo con la parte judicial, ya que la Corte Constitucional colombiana sí se ha encargado de estudiar y definir el derecho a la propia imagen, catalogándolo como un derecho autónomo e independiente de otros, que se ve lesionado simultáneamente con otros derechos como la intimidad, el honor y el buen nombre, y está directamente vinculado a la dignidad humana y la libertad.

Por ello, resulta importante para este estudio revisar las sentencias más relevantes sobre este tema así:

En primer lugar, se tiene la Sentencia T-634 de 2013 donde la Corte Constitucional sobre el derecho a la propia imagen, precisó sus características señalando que:

...El derecho a la propia imagen, a partir de los diversos aspectos desarrollados por la jurisprudencia constitucional, (i) comprende la necesidad de consentimiento para su utilización, (ii) constituye una garantía para la propia imagen como expresión directa de la individualidad e identidad de las personas, (iii) constituye una garantía de protección de raigambre constitucional para que las características externas que conforman las manifestaciones y expresiones externas de la individualidad corporal no puedan ser objeto de libre e injustificada disposición y manipulación de terceros, (iv) es un derecho autónomo que puede ser lesionado junto con los derechos a la intimidad, a la honra, al buen nombre de su titular, y cuyo ejercicio está estrechamente vinculado a la dignidad y libertad de la persona, (v) implica la garantía del manejo sobre la propia imagen cuyo ejercicio se traduce en una manifestación de la autodeterminación de las personas, y (vi) exige que las autorizaciones otorgadas para el uso de la propia imagen en el marco de la libertad en las relaciones contractuales no sean entendidas como una renuncia al derecho mismo... (T-634/2013, 2013).

Otra sentencia importante es la T-280 de 2022 porque en ella definió el derecho a la propia imagen como la facultad exclusiva de un individuo de disponer de su apariencia, voz, nombre y rasgos físicos, impidiendo que terceros los capten, reproduzcan o difundan sin autorización, precisando que nace del reconocimiento de la individualidad e identidad.

La jurisprudencia ratificada en fallos como la sentencia T-339 de 2022 y T-280 de 2022 indica que este derecho protege tres dimensiones o facetas:

...La *primera faceta* expresa la autonomía de las personas para determinar su propia imagen. Ello implica una decisión sobre la forma como se quieren ver y como quieren ser percibidas por los demás. Se trata de la autodeterminación de los individuos para diferenciarse físicamente o referirse a sí mismos en función de ciertas actividades (p.ej., intereses o profesión). Esta faceta: “puede ser comprendida como el aspecto estético o somático del derecho o la dimensión de autodefinición del ser, al tener en cuenta para definir la individualidad de la persona su imagen física, su nombre o su voz”.

La *segunda faceta* incluye un aspecto positivo y otro negativo. El primero (*positivo*) se refiere a la potestad de la persona para decidir las partes de su imagen que pueden ser difundidas de manera onerosa o gratuita. De manera que el derecho a la imagen cuenta con una faceta *exclusivamente patrimonial*. Esta se encuentra relacionada con la autorización de la explotación sujeta a la obtención de lucro y el resarcimiento económico derivado del uso y el aprovechamiento de la imagen sin el permiso de su titular. La Corte Constitucional se ha abstenido de definir las controversias relacionadas con esa faceta por no ser de su competencia. Por esa razón, el tribunal indicó que, cuando se vulnera el derecho a la imagen: “el resarcimiento de perjuicios se libra a la decisión de la jurisdicción

ordinaria” porque la tutela no es el mecanismo idóneo para solicitar una eventual indemnización o reparación de esos daños.

La *tercera faceta* incluye la *imagen social*. Esta comprende la caracterización que una persona logra de sí misma en la sociedad y que le permite identificarse plenamente frente a los otros. Con respecto a la tercera faceta, el tribunal resaltó que: “la Constitución Política protege el derecho a la imagen, no solo en lo que se refiere al aspecto físico, sino también frente a la identidad constituida por las particularidades y circunstancias concretas en las que una persona desarrolla su existencia... (T-280/2022, 2022).

Por último, en la Sentencia T-289 de 2023 se indica las dimensiones y el ámbito de protección del derecho fundamental a la intimidad, determinando que se puede clasificar en dos, una positiva y una negativa:

...La primera establece una prohibición de cualquier intervención arbitraria en la esfera privada de las personas e “impide la divulgación injustificada de hechos o documentos privados sin la autorización del titular”; y la segunda, “protege el derecho de toda persona a tomar las decisiones que conciernen a la esfera de su vida privada y desarrollar su personalidad de forma autónoma.” En ese sentido, la Corte ha establecido que el derecho a la intimidad le impone al Estado el deber de abstenerse de interferir en la vida privada y la obligación positiva de adoptar las “medidas normativas, judiciales y administrativas para asegurar el respeto de las diferentes dimensiones del derecho” (T-289/2023, 2023).

La anterior sentencia marca unas reglas de protección contra la vulneración del derecho a la propia imagen y la intimidad personal, y prohíbe la difusión no autorizada de contenido multimedia en las redes sociales actuales, determinando que el uso de la imagen ligada al contexto personal (orientación sexual, ubicación, etc.) viola de forma flagrante la dignidad humana.

En conclusión, judicialmente se ha logrado, en Colombia, una verdadera conceptualización y determinación del derecho humano a la propia imagen, la cual permite establecer cuáles son los mecanismos que se han establecido para su protección.

1.2. Derecho humano a la propia imagen en Brasil

En Brasil el derecho humano a la propia imagen deriva de la protección de datos personales que se constitucionalizó mediante la Enmienda Constitucional 115/2022 que añadió el inciso LXXIX al artículo 5 de la Constitución Federal, garantizando el derecho a la protección de datos personales incluso en medios digitales y otorgando competencia exclusiva a la Unión para legislar sobre la materia, dando así, un alcance en garantizar el cuidado de los datos personales en rango de derecho fundamental.

Esta enmienda consolidó un proceso iniciado con la Ley General de Protección de Datos (Presidencia de la República Federativa de Brasil, 2018), que establece principios de finalidad, minimización de datos y medidas de seguridad, y regula el tratamiento de datos personales y sensibles.

La Constitución Federal de 1988 otorga la máxima protección a estos derechos mediante dos pilares fundamentales:

- Artículo 5º, Inciso X: Declara inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurando el derecho a indemnización por daño material o moral derivado de su violación (Asamblea Nacional Constituyente, 1988).
- Enmienda Constitucional 115 (2022): Elevó la protección de datos personales, incluidos los medios digitales, y fue ranqueados como derecho fundamental autónomo en la Constitución (Presidencia de la República Federativa del Brasil, 2022)

La Ley General de Protección de Datos en Brasil clasifica los datos sensibles como la etnia o raza, las orientaciones sexuales y la religión que se profesa, los partidos políticos, datos de la historia clínica en salud, información genética y biométrica con reglas más estrictas que los datos personales ordinarios, reconociendo su potencial discriminatorio y su vinculación con la protección de la identidad y el libre desarrollo de la personalidad.

Por último, el marco brasileño se complementa con el Código de Defensa del Consumidor (Ley 8.078/1990), que en sus artículos 6 y 43 establece el derecho del consumidor a acceder y corregir sus datos, y con el Código Civil de 2002, cuyo artículo 927 establece responsabilidad civil por daños causados por actos ilícitos, creando un microsistema integrado de protección.

1.3. Relación con la protección de la identidad personal

La relación que deriva entre el derecho humano a la propia imagen y la identidad personal se concreta en que, esa personalidad jurídica (Art. 14) que se puede desarrollar libremente (Art. 16) incluye la imagen propia como tal, la del rostro y composición física de la persona, que no pueden ser utilizada para fines ilegales, y de la protección de uno deriva la del otro, porque pueden ser víctimas del mismo ataque virtual que se investiga.

En palabras de la Corte Constitucional colombiana “El derecho a la propia imagen, a partir de los diversos aspectos desarrollados por la jurisprudencia constitucional (...) constituye una garantía para la propia imagen como expresión directa de la individualidad e identidad de las personas” (T-634/2013, 2013), entonces, como quiera que la imagen es uno de los principales componentes de la identidad personas, el ataque a este implica la afectación de la identidad personal en su conjunto.

Por ello es que, a continuación, se estudiará cómo es que la Inteligencia Artificial a través de sus avances ha impactado este derecho, de qué formas y cuáles son los fenómenos que han surgido al respecto.

2. Impacto de la inteligencia artificial en la comisión de conductas punibles. Comparación entre Colombia y Brasil

En este aparte, se iniciará con la conceptualización de lo que se debe entender por Inteligencia Artificial, ya que ello permitirá determinar sus alcances (positivos y negativos) para

poder mirar los ilegales, los fenómenos que surgen de su mal uso y cómo derivan en la comisión o facilitación del crimen.

Seguidamente se mirará el impacto de estos fenómenos negativos de inteligencia artificial en Colombia y Brasil.

2.1. Definición de inteligencia artificial y su uso ilícito

Colombia tiene una definición legal de Inteligencia Artificial en su normatividad vigente, que se fundamenta en el Marco Ético para la Inteligencia Artificial de 2021, que fue elaborado por el Ministerio de Ciencia, el cual funciona como una guía de *soft law* con recomendaciones no obligatorias para entidades públicas. En este documento, se define la Inteligencia Artificial como:

Un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o con seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos (Departamento Administrativo de la Presidencia de la República de Colombia, 2021).

Este documento se creó para facilitar la implementación de la Política Nacional para la Transformación Digital e Inteligencia Artificial (CONPES 3975), que establece cuatro objetivos específicos y catorce acciones orientadas a crear un nicho de Inteligencia Artificial y una estructura ética en su proceso.

También se le ha concebido como “la capacidad de las máquinas para utilizar algoritmos, aprender de los datos y tomar decisiones de manera similar a los seres humanos” (Jondec Briones, 2024), resaltándose así que busca emular el comportamiento humano.

No obstante, esa finalidad loable del mecanismo, y como quiera que el mundo digital es un reflejo del mundo real, los sistemas de Inteligencia Artificial tienden a adoptar los sesgos y rasgos de su creador, llevando a que aspectos como el racismo, la xenofobia, la homofobia, la violencia de género, así como los delitos patrimoniales, por mencionar algunos ejemplos de problemas de la sociedad actual, se diversifique y fortalezcan mediante el uso de herramientas tecnológicas como la mencionada.

Ejemplos de ello, son los presentados por la Dra. María Magdalena Sarraute Requesens en la palestra titulada “Violencia de Género digital en América Latina” el 27 de agosto de 2026 en la Seminario Certificado en la Pontificia Universidad Católica do Rio de Janeiro PUC Rio, donde recordaba cómo plataformas como chat gpt y otras, al pedírsele que generara imágenes de humanos, predeterminadamente generaba solo la de hombres de tez blanca, o el de la Dra. Agnes Christian en la palestra “Protección de datos personales e inteligencia artificial: desafíos jurídicos actuales” en el mismo evento, donde recordaba como dato similar que, si se le pedía a una plataforma de IA generar la imagen de un brasileño, lo generaba con tez oscura.

Entonces, la tecnología por sí sola no conlleva necesariamente la vulneración de los derechos humanos de las personas por medio de la comisión de conductas punibles. Sin embargo,

siempre que todas las narrativas desafortunadas que habitan el mundo real se trasladan a ese mundo artificial, se tergiversa su finalidad y caen en la criminalidad.

En cuanto a los usos ilícitos de la Inteligencia Artificial, se tiene que:

La IA genera preocupación y temor, debido a su capacidad para distorsionar de manera errónea e incorrecta la realidad, por lo que es necesario frenar estos actos antes de que adquieran más poder y provoquen trastornos sociales. Además, la manipulación y los riesgos asociados con la IA también se utilizan para causar daño personal. Uno de los riesgos más graves es los ataques cibernéticos y la ingeniería social, en los que ciertas personas crean perfiles falsos, mediante algoritmos automáticos, utilizando datos reales, y estos perfiles, posteriormente, llegan a ser manipulados para acceder a datos personales y contraseñas de otros usuarios. Por último, existe el riesgo de la manipulación de imágenes, videos o textos, que pueden ser reutilizados y clonados.

Es verdad que los beneficios de la IA son notoriamente útiles en diferentes ámbitos. Sin embargo, existe un gran número de usuarios que suelen usarla con fines ilegales, como la desinformación dirigida a diversos sectores de la sociedad. En muchos casos, hay un conocimiento limitado sobre el uso de las nuevas tecnologías, y para el usuario promedio resulta difícil distinguir entre lo verdadero y lo falso. (Jondec Briones, 2024)

Entonces, las modalidades de uso indebido de dicha tecnología son múltiples, tales como la ciberdelincuencia automatizada, ingeniería social y phishing avanzado, desinformación, cyberbullying y el llamado grooming. Esta última modalidad es preocupante, pues se trata, de un adulto, quien, por medio del uso de redes sociales, se hace pasar por un menor de edad, para contactar a menores de edad con el fin de cometer conductas punibles.

No obstante, uno de los más importantes de cara a la afectación del derecho humano a la propia imagen es el de las *deepfakes*; *por ello*, resulta importante profundizar al respecto, para efectos de determinar las medidas de intervención estatal que se han generado y que se pretenden contrastar.

2.2. Definición de deepfakes y explicación como fenómeno de la inteligencia artificial

Los *deepfakes* son contenido sintético generado por inteligencia artificial que combina el aprendizaje profundo (deep learning) con técnicas de falsificación para producir imágenes, videos o audio hiperrealistas difíciles de distinguir de material auténtico. Esta tecnología utiliza redes generativas adversariales (GAN) para superponer el rostro de una persona sobre el cuerpo de otra, creando representaciones falsas convincentes.

El término *deepfake* es un acrónimo de *deep learning* y *fake*, y se conoció a finales del año 2017 cuando un usuario de Reddit empezó a publicar videos pornográficos con rostros de celebridades superpuestos, con el avance de la tecnología digital, incluso al punto de que cualquier persona con habilidades computacionales básicas puede crear contenido pornográfico que retrata a individuos en actos sexuales que nunca ocurrieron. (Schwartz, 2018)

Los *deepfakes* se clasifican en varios tipos: foto de intercambio de rostro y cuerpo, audio de intercambio de voz, texto a voz, video de intercambio de rostro, morphing facial, puppetry corporal y sincronización labial audio-video. (Jan Kietzmann et al, 2020)

El contenido pornográfico no consentido es el uso más extendido y dañino, afectando desproporcionadamente a mujeres y violando derechos a la dignidad, privacidad y reputación, este aspecto se analiza a profundidad en el libro denominado “Fronteras Digitales y Violencia de Género: Un Estado del Arte en América Latina”, escrito por varios autores entre estos, la Doctora María Magdalena Sarraute Requeses, ya que en su intervención y presentación del pasado 27 de agosto de 2026, en la Universidad Pontificia Universidad Católica de Rio de Janeiro, resaltó aspectos relevantes que se deben ser mencionados en este artículo como por ejemplo: normas sobre violencia de género digital, Ley 12737 de 2012 y la Ley Carolina Dieckmann, que sanciona el acceso no autorizado a dispositivos electrónicos (Sarraute, et al.,2025).

La Corte Constitucional colombiana, por su parte, no ha fallado casos específicos sobre *deepfakes*, pero ha sentado precedentes sobre protección de la imagen en contextos análogos. En un caso de fotografías íntimas compartidas sin consentimiento, la Corte encontró violación de los derechos a la imagen personal y a su privacidad, ordenando al infractor abstenerse de repetir la conducta y eliminar las copias; sin embargo, la Corte reconoció que para las imágenes ya diseminadas en el mundo digital era imposible deshacer este daño, evidenciando la ineffectividad de los remedios constitucionales frente a la viralidad del contenido digital, y este deja una huella digital imborrable. (T-339/2022, 2022)

En lo que tiene que ver con la desinformación, la misma opera normalmente en temas políticos en épocas electorales, lo que pone en alerta a las autoridades y legisladores sobre la necesidad urgente de legislar sobre el tema. Ahora si bien es cierto, estas modalidades son graves, son las *deepfakes* sexuales, el mayor porcentaje de casos de uso ilícito de la IA. Por lo que, es importante ahondar en el estudio de dicha modalidad en los países a contrastar.

2.3. Impacto de la IA en la comisión de conductas punibles en Colombia

Precisados en el aparte inmediatamente anterior, los posibles usos ilícitos de la inteligencia artificial, especialmente el conocido como la Deepfake – ultrafalso-. Que nace como un mal empleo de tecnologías autogenerativas de contenidos (Deep Synthesis), en la utilización de técnicas de aprendizaje profundo (Deep learning) (Consejo Nacional de Política Económica y Social, 2025), en múltiples escenarios. Resulta importante estudiarlos a profundidad en el caso de la violencia sexual, por ser un ámbito donde ha crecido exponencialmente ese peligro en la sociedad actual, aunado a que, si bien, las demás modalidades arriba definidas de uso malicioso de la IA, pueden llegar afectar el derecho humano a la imagen propia, aquellas que simulan contenido sexual no consentido, afectan no solo a dicho derecho, sino a la dignidad y libre desarrollo de la personalidad de las víctimas.

Ahora bien, uno de los factores que se logra divisar, en ese crecimiento exponencial, es que generalmente las creaciones artificiales de imágenes por parte de la IA, tienden a enfocarse en

material con contenido sexual simulado. Adicionalmente, las principales víctimas con la creación de ese tipo de contenidos son las mujeres y niñas.

Así lo resaltó la profesora Rodríguez Pulecio, en el artículo titulado “Deepfakes: la inteligencia artificial como nueva herramienta de violencia contra mujeres y niñas”, donde, citando a Laffier & Rehman, afirmó que “La evidencia académica es clara: algunos autores explican que el 90% de las imágenes generadas por la IA son de carácter sexual y afectan de manera desproporcionada a mujeres y niñas”. (Laffier y Rehman, 2023; Lazard et al., 2025)” (Rodríguez Pulecio, 2026)

Otro factor a tener en cuenta, aunque existen estudios, como los adelantados por el proyecto de investigación DiViSAR, de la Universidad Complutense de Madrid, España, permite concluir que, a pesar de que los hombres jóvenes residentes en ese país presentan tasas más altas de victimización en cuanto a la alteración de imágenes con el uso de IA, son las mujeres las principales víctimas de ataques con ese tipo de contenido.

Concretamente, en el artículo menciona lo siguiente:

En distintos estudios, algunos finalizados y otros en marcha, realizados por nuestro proyecto de investigación DiViSAR, hemos podido constatar que los chicos jóvenes (16-29) residentes en España tienen tasas más altas de victimización por alteración digital de imágenes usando IA que las chicas de su misma edad. Y que ellos son también los perpetradores. De hombre a hombre. No obstante, en nuestro trabajo en plataformas digitales como Telegram hemos hallado que son las mujeres las principales víctimas de estos ataques. Seguimos trabajando por desentrañar las cualidades de estos abusos y sus impactos desde una perspectiva interseccional (Gutiérrez y García, 2025).

De otra parte, la necesidad de enfatizar en el estudio del tema sexual nace porque existen posturas divididas en si se debe tipificar como delito autónomo o basta con enmarcarlas en alguna de las conductas punibles existentes. Y es que, existen voces en el sentido de que esa creación de contenido sexual simulado con el uso de la IA, no consentido, no corresponde a una clase de pornografía, sino corresponde a un tipo de violencia sexual, especialmente dirigidas contra mujeres y niñas. Así lo señalan, los doctores Jacinto Gutiérrez Lorca y Elisa García Mingo en el texto titulado “Llamémoslo por su nombre: los *deepfakes* sexuales no son pornografía, sino violencia sexual”, donde al respecto indicaron:

Por otro lado, aunque es habitual leer o escuchar referirse al contenido sexual alterado como “pornografía”, estas imágenes no deberían ser etiquetadas de esta manera. Las imágenes sexuales deepfake son la prueba de que se ha cometido un abuso sexual en el que se han sustraído imágenes de una persona, editado y vejado su cuerpo usando tecnología, y que provoca daños reales a las víctimas (Gutiérrez y García , 2025).

De la anterior posición se puede deducir que no basta encuadrar las deepfakes sexuales como mera pornografía, sino que este fenómeno debe tener una conceptualización y tratamiento jurídicos más adecuados, donde se promueva la protección de los derechos de las víctimas,

otorgándole la real connotación que tiene, por lo que debe ser tipificada como un tipo de violencia sexual.

Retomando, otra de las evidencias que este tipo de fenómeno tecnológico viene en aumento, son las mediciones expuestas en el Documento Conpes 4144 de fecha 14/02/2025, donde, desde una perspectiva general de la conducta, es decir, no solo en materia sexual, asevera:

Este tipo de usos puede acarrear la utilización indebida de datos personales tanto para suplantación personal, como para la generación de este tipo de contenidos. Para el primer trimestre de 2024, en Colombia se ha evidenciado un crecimiento del 433 % respecto del número de incidentes relacionados con fraude mediante utilización de *deepfakes* (Sumsu, 2024). (Consejo Nacional de Política Económica y Social, 2025)

Este aumento en los casos de este uso malicioso de la IA no afecta solo a Colombia, sino que se trata de una problemática que va más allá de las fronteras nacionales, impactando otros países como México y España. Donde, a manera de ejemplo, casos de alto impacto mediático como los ocurridos en el Instituto Politécnico Nacional y Almendralejo, respectivamente, permiten visualizar en casos concretos cómo se materializa la vulneración del derecho humano a la propia imagen.

Al respecto, vale la pena analizar más de cerca dichos casos.

México: En el año 2023 ocho víctimas denunciaron penalmente a un estudiante del Instituto Politécnico Nacional de ciudad de México, por, entre otras modalidades, la creación de *deepfakes* Porn, donde fueron creadas imágenes falsas con contenido sexual explícito con la cara de las víctimas, y dicho material era comercializado en la plataforma Telegram (Rodríguez, Acusado un universitario de alterar con inteligencia artificial miles de imágenes de alumnas para venderlas como pornografía, 2023). Una vez capturado el señalado responsable, fueron encontradas cerca de veinte mil imágenes con este tipo de contenido. Las denunciantes eran compañeras del agresor, todas mujeres jóvenes, incluso algunas menores de edad. El caso a la fecha cuenta con sentencia condenatoria emitida el pasado 14/05/2025, donde al responsable “Diego N” le fueron impuestos cinco años de prisión y pena de multa al ser hallado responsable del delito de trata de personas en la modalidad de almacenamiento de pornografía infantil. (Rodríguez, Sentenciado a cinco años de prisión Diego N, ex alumno del IPN, por el delito de pornografía infantil, 2025)

Si bien, en este caso fue posible la judicialización del responsable, también permitió vislumbrar la falta de regulación respecto a delitos de violencia digital con inteligencia artificial. Es decir, tal flagelo no se encuentra tipificado, lo que llevó a evidenciar las limitaciones procesales y lagunas legales en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y el Código Penal Federal. Tal situación conllevó la presentación de reformas legales en dichas normas.

En el mismo, se pudo entrever que el problema, además de legislativo, es probatorio, pues se logró establecer la posesión del material pornográfico, mas no se pudo probar que el denunciado lo hubiese creado utilizando IA. (Rodríguez Pulecio, 2026)

En dicho país, la discusión sigue abierta, sin embargo, al menos ya se hace parte de la agenda nacional.

España: Quince menores de edad fueron procesados por los delitos de pornografía infantil y delitos contra la integridad moral, por manipular imágenes de al menos 20 niñas domiciliadas en el municipio de Almendralejo, en España. Este caso salió a la luz en el año 2023, y se trató del primer caso mediático de pornografía infantil creada con IA. Las fotografías reales de las víctimas fueron tomadas de fotos de perfil de WhatsApp e Instagram, y luego manipuladas por un programa de IA para que las menores aparecieran desnudas o situaciones con contenido sexual explícito. En este caso, las víctimas no solo son mujeres sino niñas, lo que agrava aún más las afectaciones del caso. El caso en la actualidad cuenta con sentencia dictada por un juzgado de menores de dicho país, que condenó a un año de libertad vigilada a 15 menores de edad, al encontrarlos responsables de 20 delitos de pornografía infantil. (Palomo, 2023).

Casos como estos han conllevado que la preocupación en España sea tan alta que ya existe regulación al respecto, es decir, protección de la imagen personal por el uso indebido de la IA, con relación al contenido de naturaleza sexual, Ley Orgánica que fue aprobada para la defensa de las Personas Menores de Edad en los Entornos Digitales. Del mismo modo que el uso de delitos ya existentes adaptados a este tipo de fenómenos, como el delito de injurias graves y contra la integridad moral. Adicionalmente, cuenta con la regulación de la Unión Europea para la IA.

Se tiene entonces, que España y Europa son pioneros no solo en la regulación del uso correcto de la IA, sino también en la regulación del material penal. Sin embargo, al igual que México, es un tema que sigue evolucionando día a día.

2.4. Impacto de la IA en la comisión de conductas punibles en Brasil -

Ahora, en el caso de Brasil, país escogido para realizar el contraste de los mecanismos penales, también se encuentra afectado por este fenómeno en el panorama de los delitos en general. La Agência Nacional de Proteção de Dados (ANPD), en su informe técnico sobre *deepfakes*, donde cita datos del Identity Fraud Report 2025–2026 de Sumsub, permitió llegar a varias conclusiones que permiten ver un panorama completo en ese país. Dicho informe, permite entrever que Brasil concentra el 39% de los casos de Deepfake detectados en América Latina durante el año 2025, siendo el principal mercado de la región latina para este tipo de fenómenos detectados. (Zago, 2025)

Asimismo, los ataques relacionados con dicha modalidad aumentaron en un 126% entre 2024 y 2025. Es llamativo que dicho aumento evidencie que otras formas de suplantación personal disminuyeron, es decir, sin acudir a la IA, pero hubo un aumento exponencial de los *deepfakes*. Ello llevó a los expertos a concluir que, el fraude tradicional ha disminuido. (Autoridade Nacional de Proteção de Dados (ANPD), 2026)

En la actualidad, la tendencia de los delincuentes es realizar menos ataques, pero sí más complejos. Esta es la principal preocupación de las autoridades, porque las herramientas de IA han llegado a un nivel de sofisticación que dificulta distinguir entre contenido real y el manipulado,

para humanos y las mismas máquinas. El fraude no se limita a la falsificación de un documento, sino a la creación de identidades sintéticas completas, que se logra combinando información verdadera con datos fabricados. Configurándose en un gran desafío para bancos, entidades financieras y plataformas digitales.

En dicho informe, la Agência Nacional de Proteção de Dados (ANPD) llamó la atención en el sentido de que esta dificultad no se queda en la creación de contenido que no corresponde a la realidad como producto final, sino que surgen inquietudes relacionadas con la obtención y el tratamiento de los datos personales con los que se alimenta a los sistemas de IA para que sean capaces de producir *deepfakes*. (la Agência Nacional de Proteção de Dados (ANPD) , 2026).

Es decir, también preocupa la obtención de esos “insumos” que requiere la IA para la creación de material falso, pues se requieren fotografías, videos, audios de personas reales, que ven cómo se accede fraudulentamente y, en la mayoría de los casos, sin autorización, a sus datos personales tomados de redes sociales privadas. Entonces el fenómeno del uso malicioso de la IA no se queda en la difusión de la falsificación, sino en la recopilación y generación de dicho material, pues en cada una de esas etapas se violentan derechos a la privacidad, a la propia imagen y a los datos personales de los ciudadanos de ambas naciones.

Adicionalmente, la Agência Nacional de Proteção de Dados (ANPD) publicó recientemente su Radar Tecnológico No. 6 “Deepfakes”, dedicado a dicho fenómeno y donde lo abordó desde diferentes perspectivas, realizando un recorrido por aristas como: los conceptos principales relacionados con dicha problemática, cómo funcionan, su relación con la protección de datos personales, su impacto en el contexto brasileño y las perspectivas a futuro.

Asimismo, en el documento también llega a la conclusión de que los principales riesgos o modalidades delictivas del uso de deepfakes en Brasil, al igual que en Colombia, con el uso malicioso de datos personales, son: suplantación de identidad, con la clonación de voz e imagen, fraudes financieros, pornografía no consentida, violencia digital y de género, manipulación electoral y desinformación, prácticas discriminatorias y racistas. (Agência Nacional de Proteção de Dados -ANPD-, 2026)

Modalidades que ya fueron conceptualizadas líneas arriba, pero cuya mención resulta importante, porque permite concluir que estamos ante un fenómeno que supera las fronteras de los países, y cuyo medio de transmisión es el ecosistema digital del que todos hacemos parte. Es decir, es un problema social, que requiere de la regulación y protección por parte de los estados.

Por último, y decantándonos por el tema de las deepfakes sexuales, hecha una revisión de casos relevantes en Brasil ampliamente documentados en la prensa del país, se observan casos recientes como los denunciados por la actriz Paolla Oliveira, quien denunció la circulación en redes sociales de fotografías y videos falsos con contenido sexual no consentido. Este ejemplo, sirve para visualizar que persiste este tipo de crímenes en contra de las mujeres, más aquellas que tienen relevancia en la sociedad. (Serra, 2026)

3. Similitudes y diferencias del Estado de Brasil y Colombia en cuanto a la forma de intervención frente a la protección del derecho humano a la propia imagen –

Revisada la cuestión de la afectación en los Estados, se puede concluir que la protección en ambos países se contempla desde el análisis del derecho a la protección de datos y que la afectación por *deepfakes* es similar como fenómeno, porque las modalidades se repiten y las suplantaciones y prácticas discriminatorias o de violencia de género digital se repiten.

En cuanto a diferencias, sí se encuentra que en Colombia el desarrollo jurisprudencial ha sido más amplio a través de normas que regulan el derecho fundamental, mientras que en Brasil el desarrollo se ha enfocado en la inclusión del derecho en la Constitución a través de enmiendas.

Por otra parte, respecto de la diferencia entre Colombia y Brasil, se tiene que se diferencian en el rango constitucional y el rango legal, para cuidar el derecho a la propia imagen, a los datos personales y a la identidad que han dado, evidenciándose así que Brasil ha avanzado más en la constitucionalización de la protección de datos; por otro lado, Colombia ha mantenido una dirección dividida.

En resumen, Brasil ha avanzado un poco más que el Estado colombiano al llevar a la Constitución la protección de datos personales, pues ha establecido el derecho autónomo; sin embargo, ambos países presentan algunos alcances limitados frente al uso ilícito de inteligencia artificial para manipular la imagen. La jurisprudencia habla de manera específica sobre esta materia en los últimos cinco años.

Precisado lo anterior, se tiene en concreto como diferencia y similitudes en lo referente al análisis del marco normativo entre Colombia y Brasil, se tiene lo siguiente:

Tabla 1. Análisis comparado entre Colombia y Brasil jurídico – penal

<i>Derecho / Aspecto concreto</i>	<i>marco normativo en Colombia</i>	<i>Marco normativo en Brasil</i>	<i>Diferencias</i>	<i>Similitudes</i>
Propia imagen	No se encuentra expresamente contemplado en la Constitución Política de Colombia de 1991, se tiene desarrollo jurisprudencial. Definió y estudió el derecho a la propia imagen. T-471 - 1999 T- 634 - 2023, T- 289-2023 y T- 280-2022 Ley 23 de 1982 Ley Estatutaria 1581 de 2012	Se encuentra expresamente contemplado en la Constitución Federal de 1988, regulado en la Enmienda Constitucional 115/2022, que añadió el inciso LXXIX al artículo 5 de la Constitución Federal. Ley General de Protección de Datos. (LGPD) Ley 13.709 de 2018	Colombia depende de la jurisprudencia de la Corte Constitucional, que desarrolló este derecho como fundamental y autónomo ligado al principio de dignidad humana. Brasil tiene normas civiles y avances legislativos directos para la protección de la propia imagen de cara a la	Los ordenamientos jurídicos penales han venido avanzando en Colombia y Brasil, en busca de la protección de la propia imagen. Colombia cuenta con la Ley 2502 de 2025; modifica el artículo 296 con la circunstancia de agravación.

<i>Derecho / Aspecto concreto</i>	<i>marco normativo en Colombia</i>	<i>Marco normativo en Brasil</i>	<i>Diferencias</i>	<i>Similitudes</i>
		Código de Defensa del Consumidor Ley 8.078/1990	inteligencia artificial, incluye la indemnización por daño material, moral o a la imagen.	Brasil tiene la Ley 15.487 del 6 de agosto de 2026.
Datos personales	Se encuentra regulado dentro del derecho fundamental al habeas data y estatus de la persona jurídica artículos 14 y 15 constitucional Ley 1273 de 2009 Ley Estatutaria 1581 de 2012	Se encuentra regulado en la Enmienda Constitucional 115/2022, que añadió el inciso LXXIX al artículo 5 de la Constitución Federal. Ley General de Protección de Datos. (LGPD) Ley 13.709 de 2018 Código de Defensa del Consumidor Ley 8.078/1990		Colombia cuenta con un bien jurídico denominado “ <i>de la protección de la información y de los datos.</i> ” Brasil cuenta con un sistema jurídico penal autónomo y específico. Ley Carolina Dieckmann
Deepfakes	Ley 2502 de 2025 introdujo una circunstancia de agravación en el delito de falsedad personal, artículo 296 C.P.	Ley 15.123 del 24 de abril de 2025. Ley 15.487 del 6 de agosto de 2026.	Colombia centra su reforma en la suplantación de identidad y el fraude y solo como agravante específico. Colombia no sanciona los <i>deepfakes</i> con contenido sexual Brasil dio un avance más significativo en agosto de 2026 en penalizar los <i>deepfakes</i> con niños y adolescentes con contenido sexual.	Ambos países, han definido el término “ <i>deepfakes</i> ”
Contenido sexual o íntimo	No se encuentra expresamente contemplado en la Constitución Política de Colombia de 1991, ni tampoco en el Código Penal	Ley 15487 del 6 de agosto de 2026, para combatir y reprimir el delito de violencia sexual contra niños o adolescentes, incluso en el entorno digital y	Colombia reconoce la difusión no consentida de material íntimo como una forma grave de violencia de género digital	Colombia tipificó la conducta recientemente con un enfoque penal muy concentrado en la órbita de delitos sexuales.

<i>Derecho / Aspecto concreto</i>	<i>marco normativo en Colombia</i>	<i>Marco normativo en Brasil</i>	<i>Diferencias</i>	<i>Similitudes</i>
		mediante el uso de inteligencia artificial.	que amerita sanción privativa de la libertad. Brasil tiene dos legislaciones que buscan la protección contra la violencia hacia la mujer en materia sexual.	Brasil contempla penalmente de manera explícita los montajes y ediciones digitales
Respuesta penal	Ley 2502 de 2025; introdujo una circunstancia de agravación en el delito de falsedad personal, artículo 296 C.P.	Ley 15.123 del 24 de abril de 2025, Brasil modificó el artículo 147-B de su Código Penal. Esta reforma introdujo una causa de aumento de la pena (hasta en la mitad) cuando la violencia psicológica contra las mujeres se cometa utilizando IA Ley 15487 del 6 de agosto de 2026, para combatir y reprimir el delito de violencia sexual contra niños o adolescentes, incluso en el entorno digital y mediante el uso de inteligencia artificial.	En Colombia existen iniciativas legislativas en el Congreso para tipificar de forma autónoma la "Creación y difusión no consentida de imágenes sexuales sintéticas", castigando la conducta sin necesidad de demostrar daño a la honra (injuria). En Brasil, la Ley 15487 del 6 de agosto de 2026, para combatir y reprimir el delito de violencia sexual contra niños o adolescentes, incluso en el entorno digital y mediante el uso de inteligencia artificial.	Ambos códigos penales optaron por el uso de circunstancias de agravación punitiva específicas en lugar de crear tipos penales independientes para la IA.

Nota: esta tabla muestra las principales semejanzas y diferencias entre la regulación normativa entre Colombia y Brasil. Información tomando la legislación vigente de Colombia y Brasil.

3.1. Intervención del Estado colombiano en general, frente a la protección del derecho humano a la propia imagen frente al uso ilícito de la IA

En cuanto a la intervención del Estado colombiano de cara a la protección del derecho humano a la propia imagen frente al uso ilícito de la IA, desde el punto de vista normativo abarca

varios ámbitos. Véase primero cómo a nivel internacional están los principios de buen uso de la inteligencia artificial, como el Reglamento de la Inteligencia Artificial expedido por el Parlamento Europeo en el año 2024, siendo este una de las regulaciones más completas y primigenias en el mundo sobre la materia.

No hay que perder de vista que, Colombia avanza desde varias aristas frente a la regulación de la IA. El documento Conpes 4144, publicado el 14 de febrero de 2025, establece la Política Nacional de Inteligencia Artificial en Colombia, del cual han sido citados algunos apartes en el presente artículo, y traza las directrices estratégicas para garantizar un uso ético y sustentable de la inteligencia artificial, para que dicha herramienta sirva para lograr la transformación económica y social del país.

El Estado colombiano para el amparo del derecho humano a la propia imagen ha tomado como base el artículo 14, 15 y 16 de la Constitución Política, los cuales pese a no tener un reconocimiento explícito del derecho a la propia imagen se entienden incorporados, puesto que conllevan una protección a la personalidad, la dignidad humana, la intimidad personal y familiar, la protección de los datos, así como el libre desarrollo de la personalidad para decidir sobre aspectos fundamentales de su imagen e identidad.

Esta línea de amparo constitucional se ha visto desdibujada en la actualidad, tras la utilización de manera ilícita de la inteligencia artificial en la creación de contenido donde se parte de una imagen, un audio o un video real, pero se manipula y se concreta en contenido o producciones audiovisuales de cosas que no corresponden a la verdad, y a esto se le denomina *deepfakes*. Esta problemática cada día más común, ha puesto a prueba la facultad institucional del Estado colombiano para proteger el derecho humano a la propia imagen, tanto en su dimensión general que vendría siendo la suplantación de identidad, el fraude, la desinformación, la reproducción de contenido falso con imágenes y características de personas reales y esto se agrava aún más si se efectúa en como en su modalidad más lesiva que es la generación de contenido sexual o íntimo no consentido con la imagen de una persona que bajo ninguna circunstancia ha aprobado la generación de este contenido.

En la práctica del amparo hasta ahora, se ha atacado desde dos frentes: primeramente, en la construcción jurisprudencial del contenido y alcance del derecho a la imagen, la cual es principalmente protegida a través de la acción de tutela y como segundo mecanismo propuestas legislativas que permanecen insuficientes para la magnitud del problema de las IA en la actualidad.

3.1.1. Intervención judicial del Estado colombiano

Como se mencionaba anteriormente, la primera intervención del Estado colombiano frente al uso ilícito de la IA no proviene de un legislador, sino de los jueces constitucionales, los cuales en la resolución de los amparos de los derechos han venido asociando la protección de la imagen con el principio de dignidad humana, de hecho, la Corte Constitucional explicó que:

el principio de la dignidad de la persona humana no sería comprensible si el necesario proceso de socialización del individuo se entendiera como una forma de masificación y

homogeneización integral de su conducta, reductora de toda traza de originalidad y peculiaridad (T-090/1996, 1996).

En la parte de la fundamentación de la decisión señaló que las características externas y sociales que identifican a una persona no pueden quedar desamparadas por el derecho, a riesgo de convertirlas en un objeto.

Esta idea, formulada hace casi décadas antes de que el Estado se enfrentara al reto de las IA, representa para el día de hoy el fundamento para resolver cualquier intervención estatal en las tecnologías que son capaces de fabricar, con similitudes casi perfectas, la voz, el rostro y el comportamiento de alguien. Así las cosas, la reacción del Estado para este momento frente al deepfake no protege solamente una imagen aislada, sino que busca que una persona y sus características no sean reducidas a un objeto manipulable por un tercero.

Así mismo, la Corte constitucional en la Sentencia T-063/2024 ha venido decantando el contenido del derecho a la imagen en tres facetas que son complementarias: 1) La autonomía para determinar la propia imagen; 2) la disposición sobre ella, esto es en sus dimensiones positiva y negativa y 3) la protección de la imagen social, que se entiende como la caracterización que la persona logra de sí misma frente a los demás. Esta sentencia afirma que cuando un tercero interfiere indebidamente en la decisión de la persona de definir cómo puede ser conocido por los demás, incurre en una falsedad o en una apropiación, explotación o reproducción no autorizada de la imagen y también interviene sin autorización en la consolidación de la imagen social del individuo titular de los derechos (T-063/2024, 2024).

Si se analiza, estos tres componentes se presentan en los *deepfakes* puesto que se está efectuando un falseamiento de la imagen y una intervención arbitraria en la imagen social del titular, de manera que la intervención estatal califica la ilicitud de la conducta independientemente de que si el uso de la IA persigue fines patrimoniales, políticos o sexuales.

En la Sentencia T-471 de 1999, la Corte hablando de la protección de los datos de una persona sostuvo que, concluido el término del contrato que autoriza el uso de la imagen “el dueño de la imagen o de la voz recupera su derecho a plenitud y, por tanto, quien la venía difundiendo queda impedido absolutamente para seguir haciéndolo, si no cuenta con el consentimiento expreso del afectado” (T-471/1999, 1999). Este parámetro fue confirmado en el presente año en 2026 en lo que corresponde a los contenidos digitales, al exigirse que el consentimiento para la divulgación de la imagen debe ser previo, libre e informado y sobre todo susceptible de ser revocado.

Así las cosas, sobre la IA generativa es directa y dicta que el consentimiento inicial otorgado por una persona para el uso de la imagen por ejemplo, para entrenar un modelo o realizar un contenido publicitario no habilita usos ulteriores no contemplados dentro de ese consentimiento, y mucho menos autoriza la generación de contenido sintético adicional, de manera que el Estado, a través del juez constitucional, ha construido en la actualidad una barrera dogmática frente a la reutilización no consentida de la imagen mediante IA, incluso antes de que existiera legislación específica sobre la materia.

A pesar de que la Corte Constitucional no se ha pronunciado todavía, sobre los límites y alcances sobre un caso específico de *deepfake*, su jurisprudencia sobre la difusión no consentida de contenidos en plataformas digitales constituye la base sobre la cual se puede solicitar la intervención estatal frente a la IA.

De hecho, en la Sentencia T-339 de 2022, la Corte señaló que exhibir fotografías íntimas de otra persona sin su consentimiento “es una conducta que tiene la capacidad de afectar, de manera evidente y manifiesta, varios derechos fundamentales de la persona” y que, además, “puede afectar la salud mental de la persona a la que se exhibe” (T-339/2022, 2022)

En ese mismo sentido, la Sentencia T-561 de 2023 tuvo como conclusión que la divulgación de imágenes ajenas en redes sociales sin autorización vulnera “los derechos a la propia imagen y a la intimidad” (T-561/2023, 2023). Lo que muestra que el fenómeno de los *deepfakes* ya tiene un marco jurisprudencial por medio del cual puede solicitarse el amparo por medio de la acción de tutela.

3.1.2. Intervención legislativa colombiana para la protección del derecho a la propia imagen frente al contenido de la IA

El ordenamiento colombiano ya contaba con herramientas jurídicas aplicables, de manera indirecta, a la suplantación digital de la imagen, antes de toda la problemática que se ha venido presentando con la IA, dentro de las cuales se encuentra la Ley 1581 de 2012 que estableció el régimen general de protección de datos personales, la cual es aplicable a la recolección y tratamiento de imágenes y datos biométricos empleados para el entrenamiento de sistemas de IA; también está la Ley 1273 de 2009 que adicionó al Código Penal el Título VII BIS “De la Protección de la Información y de los Datos” donde se clasificaron comportamientos, como por ejemplo el delito de acceso abusivo a sistemas informáticos y la violación de datos personales. Pese a lo anteriormente expuesto, ninguna de estas normas fue concebida específicamente para enfrentar la creación de contenido audiovisual sintético, lo que ha estado generando un vacío punitivo para los *deepfakes* a los que nos enfrentamos en la actualidad.

Ahora bien, la respuesta legislativa más significativa del Estado colombiano frente al fenómeno de los *deepfakes* es la 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” la cual su principal mérito es introducir, por primera vez en el ordenamiento penal colombiano, definiciones normativas de conceptos hasta entonces ausentes del lenguaje legal en donde el *deepfake* es definido como “la creación, modificación y utilización de un registro audiovisual, incluidas fotografías, vídeos, imágenes o grabaciones de sonido falsos, mediante Inteligencia Artificial [...] de manera que el registro parezca auténtico del discurso o conducta real de un individuo” y la imagen la define como “la proyección externa de una persona, que incluye aspectos físicos, como el rostro, la voz y el cuerpo, así como aspectos emocionales y reputacionales” (Congreso de la Republica de Colombia, 2000).

Esta ley más allá de su dimensión punitiva impone al Gobierno Nacional, a la Fiscalía General de la Nación, a la Policía Nacional y al Ministerio de Justicia y del Derecho, la obligación de formular una política pública sobre el uso de la IA que contemple un marco ético, la educación

digital, el desarrollo de herramientas forenses de detección de deepfakes y protocolos de respuesta rápida pero es algo que permanece en gran medida por desarrollar.

3.1.3 La intervención del Estado frente al uso ilícito de la IA en contenido sexual e íntimo

La forma más lesiva del uso ilícito de la IA sobre la propia imagen en la actualidad es la generación de contenido sexual o íntimo no consentido, en la cual la intervención del Estado colombiano hasta ahora ha sido insuficiente por ser meramente judicial, de hecho, el pronunciamiento más relevante en la materia es la Sentencia T-184 de 2026, en la que la Corte desarrolló la categoría de “violencia digital”, entendida como una continuidad de la violencia estructural contra las mujeres en el entorno virtual, allí respecto del consentimiento, la Corte dio la precisión de que este “debe otorgarse siempre libre de contaminación, coacción o engaño” y que “cualquier tipo de artificio con la vocación de coartar la libertad de decidir debe ser censurado” (T-184/2026, 2026).

La referencia tácita al “artificio” como un elemento que es capaz de viciar el consentimiento resulta especialmente importante frente a los deepfakes sexuales, en la medida en que estos constituyen, por definición, un artificio tecnológico que impide a la persona representada ejercer cualquier forma de autodeterminación sobre su imagen y es absolutamente gravosa para quien lo enfrenta. En esa misma providencia, la Corte realizó un ejercicio de derecho comparado bastante ilustrativo para evaluar la suficiencia de la intervención estatal colombiana, de hecho señaló que en México, a raíz del caso de una mujer que “se enfrentó con un vacío normativo y una respuesta institucional que no reconocía dicha conducta como delito”, se expidió la Ley Olimpia, que adicionó al Código Penal Federal un título de “Delitos contra la Indemnidad de la Privacidad de la Información Sexual” y además señaló que España incorporó desde 2015 el delito de difusión no consentida de imágenes íntimas para “poner fin a una relevante laguna de punición”, así mismo expresó que Perú tipificó en 2017 una conducta similar, calificándola como “un tipo de violencia psicológica, doméstica e incluso como una forma de abuso sexual” (T-184/2026, 2026).

El anterior recuento comparativo constituye por parte del juez constitucional una exhortación implícita al legislador colombiano para que mediante tipos penales autónomos pueda llenar vacíos que la experiencia ya identificó como problemáticos.

Sin embargo, la legislación colombiana aún no ha seguido todavía el camino del derecho comparado, toda vez que la Ley 2502 de 2025 circunscribe el agravante exclusivamente al delito de falsedad personal, sin contemplar un tipo penal autónomo para los deepfakes de contenido sexual no consentido, modalidad que concentra la mayoría de los casos reportados a nivel global y que afecta desproporcionadamente a las mujeres y esta omisión resulta especialmente preocupante si se considera que la propia Corte Constitucional calificó la difusión no consentida de contenido íntimo como una forma de violencia sexual y de género que exige “medidas necesarias para prevenir, proteger, reparar, prohibir y penalizar los comportamientos que configuren una violencia de género digital o en línea” (T-184/2026, 2026).

A diferencia de México, España y Perú, Colombia no tiene regulado todavía con un tipo penal autónomo e independiente que sancione o regule específicamente la creación o difusión de deepfakes de contenido íntimo sin consentimiento, de manera que la intervención estatal frente a

esta modalidad continúa casi en su totalidad, siendo amparada por la acción de tutela y la doctrina jurisprudencial reseñada.

En consecuencia y, a manera de conclusión se tiene que la intervención del Estado colombiano frente al uso ilícito de la IA sobre el derecho humano a la propia imagen, entonces presenta una asimetría clara ya que mientras el desarrollo jurisprudencial ha construido un marco doctrinal robusto que se encuentra fundado en la protección de la dignidad humana, las tres facetas del derecho a la imagen y la revocabilidad del consentimiento, la intervención legislativa sigue siendo puntual e insuficiente, tanto en su dimensión general como, sobre todo, frente al contenido sexual no consentido. De hecho, esta insuficiencia se proyecta también sobre la responsabilidad de los intermediarios digitales porque la Corte ha reconocido que, si bien las plataformas no son, en principio, responsables por los contenidos publicados por terceros, “sí deben garantizar un mecanismo real, serio y oportuno” para la protección de sujetos históricamente discriminados según la Sentencia T-184/2026, criterio jurisprudencial plenamente aplicable para estos casos de deepfakes, en los que la velocidad de la difusión digital hace que el daño se torne, en no pocas ocasiones, irreparable. En consecuencia, la intervención del Estado colombiano debe profundizar en al menos tres frentes como lo son, la tipificación autónoma de los deepfakes de contenido íntimo no consentido, el fortalecimiento de mecanismos ágiles de remoción de contenido y de responsabilidad de plataformas digitales, y el desarrollo efectivo hoy todavía pendiente de la política pública de IA ordenada por la Ley 2502 de 2025.

Ahora, en materia penal, la intervención del Estado puede ser observada desde dos puntos de vista, uno de los delitos en general y dos de aquellos relacionados con el uso malicioso de la IA en delitos sexuales, cometidos, como viene visto, en su mayoría contra mujeres y niñas.

3.1.4. Deepfakes en materia penal sexual en Colombia

Tal como se ha visto, el Deepfakes en materia penal es un modelo delictual en pleno auge en todo el mundo y Colombia no escapa a dicha realidad. En esta tendencia, son mujeres y niñas las principales víctimas de este tipo de flagelos. Es posible realizar esa afirmación, si observamos las estadísticas reportadas en el Documento Conpes 4144 del 14 de febrero de 2025, por el Departamento Nacional de Planeación, cuando afirma: “Finalmente, es importante subrayar que la generación de contenido falso usando sistemas de IA afecta particularmente a mujeres y niñas.” (Consejo Nacional de Política Económica y Social, 2025, pág. 67).

Es la desinformación y la difamación, mediante Deepfakes, las principales modalidades de violencia en internet contra las mujeres. Adicionalmente, dicho documento revela que: “A lo anterior, hay que sumar que alrededor del 95 % de los deepfakes en internet son de contenido sexual no consentido, lo cual afecta a las víctimas en múltiples dimensiones de su vida (Fundación Karisma, 2023)” (Consejo Nacional de Política Económica y Social, 2025, pág. 67)

Idéntica denuncia, también fue hecha por la doctora María Magdalena Sarraute Requesens, en su palestra titulada “Protección de Datos Personales e Inteligencia artificial: desafíos jurídicos actuales”, quien insistió que son las mujeres las principales víctimas de violencia de género en línea, no solo en Colombia, sino en toda américa latina.

Por ello resulta importante verificar, cual es el alcance de la protección legal y jurisprudencial en Colombia para este tipo de delitos.

Al respecto, la Sala Penal de la Corte suprema de justicia en Sentencia SP2545-2020, dentro del proceso radicado No. 52010 reconoce la existencia de un vacío normativo frente a la creación de material con contenido sexual con el uso de IA no autorizado, ya que precisa que no son punibles conductas como la pornografía infantil técnica, la pseudopornografía y la pornografía infantil artificial, porque el Art. 218 del Código Penal sanciona el fotografiar, filmar, grabar, producir, divulgar, ofrecer, vender, comprar, poseer, portar, almacenar, transmitir o exhibir, por cualquier medio, para uso personal o intercambio, de representaciones sexuales que involucren personas menores de 18 años, solo en los eventos de que estas sean reales.

Dicha providencia señala;

En este aspecto, nuestra legislación difiere de las que amplían el concepto de pornografía, al material elaborado especialmente por medios informáticos, en el que se manipulan las imágenes de manera que, a los protagonistas, siendo personas mayores de edad, se les da la apariencia de niños, o incluso penalizan el material que revela personajes ficticios, que asemejan a reales, realizando comportamientos sexualmente explícitos. Por consiguiente, en acatamiento de los principios de legalidad y estricta tipicidad, sin que haya lugar a extender la norma a aspectos no contemplados previamente por el legislador, las siguientes modalidades de pornografía no son punibles en el ordenamiento nacional: i) la pornografía infantil técnica, en la que intervienen personas que no tienen la condición de ser menores de edad, pero que aparentan serlo, bien porque físicamente parecen tales, o porque mediante recursos tecnológicos se les da esa apariencia; ii) la pseudopornografía, en la cual se insertan fotogramas o imágenes de menores reales en escenas pornográficas en las cuales no intervinieron realmente, lo cual significa que no fueron abusados; y iii) la pornografía infantil artificial, en la que intervienen menores creados a partir de un patrón irreal, ya sea por dibujos o animaciones de todo tipo, es decir, no representan a un ser humano con existencia real (SP2545-2020 , 2020).

Ahora, si bien es cierto, según nuestra interpretación, la corte reconoce el vacío normativo en materia de creación de contenido sexual mediante el uso de la IA sin autorización, también lo es que existen normas generales que regulan el tema, pero no concretamente en el tema sexual. Uno de ellos es el agravante contemplado para el punible de violación de datos personales, el cual fue introducido por la Ley 2502 de 2025, la cual modificó y adicionó el artículo 296 del Código Penal, con un inciso donde estipula que cuando se hace el uso de la utilización de Inteligencia Artificial para falsear según este delito, la multa se aumentará hasta en una tercera parte, siempre que la conducta no constituya otro delito.

Adicionalmente, el texto denominado Fronteras Digitales y Violencia de Género, Un Estado del Arte en América Latina, cuya coautora es la Doctora María Magdalena Sarraute Requesens, ponente de la Palestra titulada: Protección de Datos Personales e Inteligencia artificial: desafíos jurídicos actuales, texto en el que se analiza, entre otros aspectos, los sistemas normativos de varios países en latino américa, entre ellos Colombia y Brasil, donde se analizaron las leyes que protegen a las mujeres de delitos de género en internet, aseveró que en la actualidad no se disponen

de recursos legales aprobados para combatir este flagelo en el ámbito digital, ellos a pesar que se han presentado varios Proyectos de Ley, como el No. 154/2019. Que, en la actualidad, dicha persecución penal se hace recurriendo a tipos penales ya existentes en el Código Penal, tales como la extorsión (artículo 244 del CP), violencia ilícita de comunicaciones (artículo 192), los cuales presentan serias limitaciones, en especial en casos de difusión de material íntimo no consentido. (Sarraute Requeses, Avendaño Paredes, Torres Zambrano, & Hidalgo López, 2025)

Obsérvese entonces cómo se evidencia que, en materia penal, las deepfakes sexuales, si bien son perseguidas por algunos tipos penales preexistentes, a la fecha no existe regulación expresa al respecto en el sistema jurídico colombiano, por lo que la misma no es delito de manera independiente, dejando al país rezagado al respecto.

3.2. Intervención del Estado de Brasil frente a la protección del derecho humano a la propia imagen frente al uso ilícito de la IA -

Brasil adopta un enfoque más estructurado. La Política Brasileira de Inteligencia Artificial (EBIA), lanzada en 2021, promueve la utilización responsable de la inteligencia artificial, fomenta la innovación y mejora la coordinación entre los distintos sectores públicos y privados.

El Proyecto de Ley 2.338/2023 establece el marco legal para el uso de IA, definiendo principios, derechos y responsabilidades, e incorporando medidas de gestión de riesgos y obligaciones de protección de datos.

En Brasil se define la IA como un conjunto de tecnologías que simulan capacidades cognitivas humanas razonamiento, aprendizaje y toma de decisiones, procesando grandes volúmenes de datos de manera autónoma o semiautónoma.

Esta definición contrasta con la ausencia de un concepto normativo en Colombia, donde el marco ético no distingue entre IA tradicional y las técnicas recientes de aprendizaje profundo (*deep learning*) que representan el mayor desafío regulatorio.

En el texto, arriba señalado, titulado: Fronteras Digitales y Violencia de Género, Un Estado del Arte en América Latina, al analizar la perspectiva de Brasil, los autores señalan que dicho país, de manera análoga o semejante a otras naciones de América Latina, viene avanzando en la incorporación de tipos penales que pueden aplicarse a la violencia digital. En dicho texto se asevera que, a pesar de los avances legislativos, la violencia digital sigue en aumento. A modo de ejemplo, la docente señaló el caso emblemático de la actriz brasileña Carolina Dieckmann, quien fue víctima de divulgación de contenido íntimo no consentido. Por ella se creó la Ley No. 12.737, del 30 de noviembre de 2012, que aborda la clasificación penal de los delitos informativos, por medio del cual modificó el Código penal brasileño, y que lleva su nombre, en la que se tipificaron delitos informáticos como el acceso no autorizado a dispositivos electrónicos (artículo 154-A). Sin embargo, resalta la docente que Brasil se queda corto en la protección y que en la actualidad NO existe un delito independiente que castigue la difusión no consentida de material sexual, en el caso de las adultas (Sarraute Requeses, Avendaño Paredes, Torres Zambrano, & Hidalgo López, 2025).

Sin embargo, al igual que en Colombia, Brasil echa mano de la legislación preexistente en el Decreto Ley No. 2.848 del 7 de diciembre de 1940, actual Código Penal Brasileño, tales como Injurias y calumnias (138 a 145), amenazas (146 y 147), persecución o acoso (147-A), acceso no autorizado a dispositivos informativos (154 -A) y Registro o montaje no consentido de contenidos íntimos o sexuales (216-B), pero no existe penalización al respecto, concluyendo la docente en que, a pesar del desarrollo en su marco legal, este vacío normativo se edifica como unas limitaciones que deben ser superadas.

Ahora, en material de menores de edad, el panorama se aclara un poco, pues con la actualización la Ley 8.069 del 13 de julio de 1990, del Estatuto del Niño y del Adolescente (ECA) , SI se criminaliza, expresamente, la simulación de un menor de edad en material sexual adulterado, con uso de la IA. Dicha sanción abarca desde el acceso a la o visualización del material, hasta su creador (Sarraute Requeses, Avendaño Paredes, Torres Zambrano, & Hidalgo López, 2025).

En el artículo 241 de dicha norma, prohíbe vender fotografías o imágenes de pornografía que involucren niños o adolescentes. 241 – A publicar o divulgar material de pornografía de niños o adolescentes. 241 – B el almacenamiento de material visual pornográfico con niños o adolescentes. 241 – C, siendo este el más importante para la materia que nos ocupa, pues se tipifica Simular la participación de un niño o adolescente en una escena de sexo explícito o pornografía mediante adulteración, montaje o modificación de cualquier medio digital.

4. posibles formas de intervención del Estado colombiano que brinden garantías de protección de la propia imagen

Como propuestas de posibles formas de intervención penal para Colombia, frente al uso ilícito de la inteligencia artificial, acudiendo a la experiencia contrastada con Brasil, se pueden delimitar las siguientes:

4.1. Implementar una circunstancia de mayor punibilidad específica para la ejecución de conductas punibles usando la IA

De lo estudiado hasta el momento, se puede concluir que Colombia y Brasil comparten un mismo problema, que consiste en que no poseen delitos específicos que sancionen expresamente los diversos uso ilícito de la IA en los eventos en que las víctimas son adultos, ya que para ello, lo que han hecho es acudir a los delitos existentes para reprocharlos, tratando de encajar cada evento en alguna conducta punible.

Esto se explica en que resulta complejo tipificar cada uso ilícito de la IA debido a que estos evolucionan rápidamente, siendo difícil prever legislativamente cual será el uso ilegal que se debe reprochar autónomamente; es que, el auge de la inteligencia artificial incentiva el utilizarla como un instrumento para la comisión de conductas punibles que pueden quedar impunes ante el vacío normativo sin ningún tipo de consecuencia.

Por ello es que, frente a esta problemática tan seria, es importante preguntarnos si ¿puede o debe el uso de la IA, en la ejecución de un delito, constituir por sí mismo una circunstancia de mayor punibilidad?

La respuesta ha de ser positiva, porque esta modalidad permitiría reprochar penalmente los futuros usos ilícitos que se lleguen a crear, superando la problemática de estar buscando la forma de tipificar cada modalidad o el estar tratando de encargar forzosamente estos fenómenos en los delitos existentes.

Ahora, la experiencia comparada de Brasil y Colombia estudiada, permite deducir que sí se hace necesario aumentar la pena cuando una conducta punible se ejecuta usando herramientas de IA porque este uso genera múltiples problemas de orden probatorio que dificulta la persecución del autor, en la medida que la experiencia actual permite deducir que solo se logra sancionar a quien tiene en su poder el material generado con IA y no a quien lo creó o lo divulgó, y este uso afecta gravemente a las víctimas por el poder de difusión y dificultad de conjurar o hacer cesar el daño generado.

Esta propuesta se podría criticar bajo el argumento de que ese uso ilícito implícitamente se encuentra previsto en otras circunstancias de mayor punibilidad existentes en el Código Penal, tales como las de los numerales 5, 8 y 17 del Art. 58, debido a que:

- El numeral 5 agrava la conducta perpetrada mediante ocultamiento, donde se podría encajar los eventos en que la IA facilita el ocultamiento del autor,
- El numeral 8 agrava la conducta de quien aumenta deliberada e inhumanamente el sufrimiento de la víctima, causando a ésta padecimientos innecesarios para la ejecución del delito, donde se podría ubicar los usos ilícitos de la IA que implican divulgaciones incontrolables de material sensible, o el grave daño a la intimidad, y
- El numeral 17 adicionado por el artículo 2 de la Ley 1273 de 2009 agrava la conducta en los eventos que “para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos” donde se podría ubicar la IA como uno de estos.

Sin embargo, tal conclusión lo único que generaría es trasladar el problema detectado para la tipificación de los fenómenos de uso ilícito de la IA a las causales de mayor punibilidad, perpetrando así el problema de no contar con un mecanismo eficaz de sanción de la conducta, e implicaría serios debates de estricta tipicidad, porque:

- El uso de la IA no puede catalogarse per se, como una maniobra de ocultamiento,
- El aumento deliberado e inhumano del sufrimiento de la víctima no permitiría sancionar esas divulgaciones no previsibles generadas por la IA, que escaparían del control del autor, o dificultaría imputarlas a alguno de los autores o partícipes en la cadena delictiva, y
- La inclusión en los medios electrónicos o telemáticos podría ser criticada bajo el argumento de que esa circunstancia fue concebida en un contexto tecnológico muy anterior a las actuales IA generativa, por lo que surgiría la duda, de si el numeral 17 resulta suficiente para cobijar dogmáticamente los supuestos de comisión delictiva mediante IA, o si la naturaleza cualitativamente distinta de estas tecnologías como lo son ahora, su capacidad de generar contenido sintético indistinguible de la realidad, que pueden operar de manera autónoma o semiautónoma, y tienen la capacidad de

escalar el daño a una velocidad sin precedentes exige un tratamiento normativo diferenciado.

También se podría presentar como crítica, que la previsión de esta circunstancia de mayor punibilidad se constituiría en una doble incriminación ante eventos como el del Art. 296 del CP, donde ya se contempló como agravante la falsedad personal que se realice con la utilización de Inteligencia Artificial, pero ello no es así porque:

- El Art. 58 del CP es claro en precisar que, las circunstancias de mayor punibilidad operan siempre que no hayan sido previstas de otra manera y
- La falsedad personal solo sanciona a quien suplanta a otro, no a quien crea contenido falso y lo divulga sin necesidad de hacerse pasar por la víctima, entonces, esta conducta punible no sería suficiente para sancionar todas las modalidades existentes y las que se han de crear de uso ilícito de la IA.

Es por ello que, aunque la Ley 2502 de 2025 da un paso inicial, sin embargo, no es suficiente de cara a aquellas las modalidades presentes de suplantación con el uso de la IA, y de hecho ha advertido que el incremento de la multa hasta en una tercera parte “tiene un valor más simbólico que práctico” frente a la magnitud del daño causado desde la perspectiva de los críticos de la ley en mención.

Lo que evidencia una tensión no resuelta por el legislador para la técnica de incorporar agravantes específicos, delito por delito, conforme vayan identificándose nuevas modalidades de comisión mediante IA, puesto que hasta el momento resulta reactiva, fragmentaria y, en última instancia, insuficiente frente a un fenómeno tecnológico transversal que puede instrumentalizarse para la comisión de prácticamente casi que cualquier conducta punible, desde por ejemplo, el homicidio facilitado mediante manipulación algorítmica de sistemas críticos hasta el fraude procesal mediante evidencia falsificada con IA, pasando por la injuria, la calumnia, la extorsión o el acceso abusivo a sistemas informáticos, entre otros.

El uso de la IA comporta una mayor lesividad y dificultad de defensa e identificación del autor puesto que, a diferencia de los medios informáticos tradicionales contemplados por la Ley 1273 de 2009, los sistemas de IA generativa permiten producir contenido falso a gran escala, de manera automatizada y con un grado de verosimilitud que dificulta su detección por parte de la víctima o de terceros.

Frente al panorama expuesto, es considerable que la técnica más adecuada de política criminal no es la multiplicación de agravantes específicos, como lo que ya fue introducido por la Ley 2502 de 2025 exclusivamente para la falsedad personal, sino que lo viable es la incorporación de un nuevo numeral al artículo 58 del Código Penal, en términos análogos a los del numeral 17 que son los medios informáticos, electrónicos o telemáticos donde se reconozca como circunstancia genérica de mayor punibilidad la ejecución de la conducta punible mediante la utilización de sistemas de inteligencia artificial, en particular cuando estos se empleen para la creación o modificación de contenido audiovisual, de voz o de datos que simule hechos, conductas o discursos no correspondientes a la realidad.

Esta vía representaría para el legislador y para el sistema de justicia en el país al menos tres ventajas frente al modelo de agravantes específicos: primero, porque se garantiza una respuesta punitiva coherente y sistemática frente a cualquier conducta del catálogo penal que se ejecute mediante IA, sin depender de que el legislador identifique, delito por delito, las modalidades de comisión facilitadas por esta tecnología tarea que, dada la velocidad del avance tecnológico, se corre el riesgo permanente de ir quedando rezagada por la realidad; en segunda medida porque se ajusta a la técnica legislativa históricamente empleada por el propio Código Penal colombiano, que ya demostró con la implementación del numeral 17 adicionado por la Ley 1273 de 2009, la viabilidad de establecer agravantes genéricos vinculados al empleo de tecnología; y en tercera medida porque le permite al juez penal valorar, en cada caso en concreto y cumplir con el artículo 58 del Código Penal que exige una fundamentación explícita sobre los motivos de la determinación cualitativa y cuantitativa de la pena, si la utilización de la IA en un caso específico incrementó efectivamente la lesividad de la conducta y en consecuencia logra evitar una agravación automática y potencialmente desproporcionada, en línea con los principios de legalidad, proporcionalidad y necesidad de la intervención penal.

Así las cosas, la implementación de una circunstancia genérica de mayor punibilidad en el artículo 58, complementada con agravantes específicos, donde la gravedad cualificada del fenómeno lo justifique, constituye, en definitiva, la intervención penal más coherente y sistemática que el Estado colombiano puede ofrecer frente a la utilización de la inteligencia artificial en la comisión de conductas punibles.

4.2 Adoptar la tipificación del Art. 241 C del Código Penal de Brasil en Colombia

Como se pudo observar en el contraste de medidas punitivas, Brasil a diferencia de Colombia, sí cuenta con un tipo penal que sanciona, a través del Art. 241 C, la simulación de la participación de un niño o adolescente en una escena de sexo explícito o pornografía mediante adulteración, montaje o modificación de cualquier medio digital.

Esta medida punitiva sería importante para Colombia, porque se ha reconocido por la Sala de Casación Penal de la Corte Suprema de Justicia que, esta clase de conductas no son punibles en nuestro sistema penal porque el Art. 218 del CP solo sanciona estas conductas cuando se trata de actividad real y no simulada.

Cabe preguntarse ¿se hace necesaria la sanción de la actividad sexual simulada de niños, niñas y adolescentes? La respuesta debe ser positiva porque, como vimos en el estudio realizado, esta actividad simulada también afecta gravemente a las víctimas, especialmente a la mujer que se le somete a la producción de deepfakes sexuales que generan graves daños en su reputación y en su psiquis, ya que es difícil entrar a explicar que se trata de montajes y el frenar esta clase de contenido se vuelve cada vez más imposible.

Por ende, esta sería otra medida que, a nivel penal se puede adoptar en Colombia, usando la experiencia de Brasil como ejemplo.

5. Conclusiones

A modo de cierre y como conclusión del presente artículo, es preciso indicar que, una vez desarrollados el objetivo específico y los generales, se logró establecer que los Estados colombiano y brasileño enfrentan una nueva era digital artificial difícil de controlar, que evoluciona rápidamente con el uso desmesurado de la inteligencia artificial frente a la comisión de conductas ilícitas. Este crecimiento exige por parte de los estados una intervención estatal que hasta este momento ha avanzado con proyectos de ley y jurisprudencia constitucional.

Una vez analizada el desarrollo jurisprudencial y normativo del derecho humano a la propia imagen en Colombia y Brasil, se logró precisar, que en el primero de los casos existe un desarrollo jurisprudencial por medio del cual se ha construido un marco doctrinal que se encuentra fundamentado en la protección de la dignidad humana, las tres facetas del derecho a la imagen y la revocabilidad del consentimiento, construyendo así una noción del derecho a la propia imagen únicamente desde el punto de vista jurisprudencial. Mientras que, en Brasil, el derecho humano a la propia imagen se observa positivizado mediante la Enmienda Constitucional 115/2022 que añadió el inciso LXXIX al artículo 5 de la Constitución Federal, otorgándole el rango de derecho fundamental.

Así mismo, luego de realizar un estudio del impacto de la Inteligencia artificial en la comisión de conductas punibles, realizando una comparación entre Colombia y Brasil, se logró concluir por mediciones hechas por instituciones públicas de cada nación, que dicho fenómeno va en aumento, ante el avance exponencial de este tipo de tecnologías, los cuales han evolucionado a tal punto de dificultar, aun a expertos, la identificación de contenido real o uno falso o ultra falso. También se logró establecer, que, aunque existen diferentes modalidades de usos maliciosos de la IA, son las Deepfakes y Deepfakes sexuales, las modalidades que mas retos representan para ambos países. Ello teniendo en cuenta los bienes jurídicos que vulnera, y que representan una nueva modalidad de violencia de género, pues son las niñas y mujeres las principales víctimas de estas conductas.

Identificada dicha problemática, y revisadas las similitudes y diferencias del Estado de Brasil y Colombia en cuanto a la forma de intervención frente a la protección del derecho humano a la propia imagen, se logró establecer que, en materia penal, en ninguno de los dos países existe un delito autónomo que penalice la creación de contenido sexual no consentido por medio del uso de la IA, en lo que adultos se trata. Ambas naciones echan mano de delitos preexistentes, para tipificar este tipo de acciones.

No obstante, si se presenta un avance significativo en Brasil, frente a la protección de niños y adolescentes, con la Ley 8.069 del 13 de julio de 1990, del Estatuto del Niño y del Adolescente (ECA), que SI se criminaliza, expresamente, la simulación de un menor de edad en material sexual adulterado, en el artículo 241 -C.

En ese orden, la intervención normativa estatal sigue siendo puntual, en consecuencia, la intervención requiere profundizar en mecanismos legislativos que den respuesta al deber del estado de prevenir y promulgar normas que den garantías de seguridad jurídica, protección de derechos humanos y garantías al principio de legalidad (*nullum crimen, nulla poena sine lege*).

Adicionalmente, se propuso como objetivo proponer posibles formas de intervención del Estado colombiano que brinden garantías de protección de la propia imagen atendiendo a principios de legalidad, proporcionalidad y necesidad de la intervención penal, revisando la experiencia brasileña que al respecto existe. Oportunidad en la que se propuso la creación e incorporación de un nuevo numeral al artículo 58 de la ley 599 de 2000 (Código Penal colombiano), donde se reconozca como circunstancia genérica de mayor punibilidad la ejecución de la conducta punible mediante utilización de sistemas de inteligencia artificial, en particular cuando estos se empleen para la creación o modificación de contenido audiovisual, de voz o de datos que simule conductas, discursos o hechos no correspondientes a la realidad.

Igualmente, se propuso implementar como delito independiente la creación de material sexual simulado que involucren a menores de edad por medio del uso de IA, debido a su condición sujetos de especial protección constitucional, tal como el previsto en Brasil, en el artículo 241- C de su Código Penal.

Así las cosas, a manera de cierre, es indiscutible de la actualidad del tema que nos ocupa. La continua evolución del fenómeno de los usos ilícitos de la IA, se caracteriza, porque la tecnología avanza mucho más rápido que las normas, lo que lleva a desprotección de derechos humanos, en este caso, a la propia imagen. Que si bien, tanto Colombia como Brasil, presentan avances en la penalización y protección de nuevos bienes jurídicos, aún los desafíos son importantes, pues en ambas naciones se observa falta de regulación normativa, quedando el reto de ponerse a la vanguardia de los nuevos retos tecnológicos.

Referencias

- Asamblea Nacional Constituyente. (22 de septiembre de 1988). Constitución Política de la República Federativa del Brasil. Brasilia, Brasil.
- Agência Nacional de Proteção de Dados -ANPD-. (2026). *informe No. 6. Deepfakes*. Brasilia, Brasil.
- Asamblea Nacional Constituyente. (20 de julio de 1991). Constitución Política de Colombia. Bogotá, Colombia.
- Autoridade Nacional de Proteção de Dados (ANPD). (2026). *ANPD publica Radar Tecnológico sobre deepfakes*.
- Congreso de la Republica de Colombia. (2000). *Ley 599 de 2000 Por la cual se expide el Código Penal*.
- Congreso de la República de Colombia. (17 de octubre de 2012). Ley 1581 de 2012. Bogotá, Colombia.
- Congreso de la República de Colombia. (17 de octubre de 2012). Ley Estatutaria 1581 de 2012. Bogotá, Colombia.
- Congreso de la República de Colombia. (28 de julio de 2025). Ley 2502 de 2025. Bogotá, Colombia.
- Consejo Nacional de Política Económica y Social. (2019). *CONPES 3975*. Bogotá.
- Consejo Nacional de Política Económica y Social. (2025). *CONPES 4144*. Bogotá.
- Departamento Administrativo de la Presidencia de la República de Colombia. (octubre de 2021). **Mar4.)** se pondrá posibles formas de intervención del Estado colombiano que brinden

- garantías de protección de la propia imagen atendiendo a principios de legalidad, proporcionalidad y necesidad de la intervención penal, revisando la experiencia brasileña que al respecto existe. co Ético para la Inteligencia Artificial en Colombia. Bogotá, Colombia. 4.) se propondrá posibles formas de intervención del Estado colombiano que brinden garantías de protección de la propia imagen atendiendo a principios de legalidad, proporcionalidad y necesidad de la intervención penal, revisando la experiencia brasileña que al respecto existe.
- Fortinet. (2026). *fortinet.com*. Obtenido de <https://www.fortinet.com/lat/resources/cyberglossary/deepfake>
- Gutiérrez Lorca, J., & García Mingo, E. (2025). Llamémoslo por su nombre: los deepfakes sexuales no son pornografía, sino violencia sexual. *Oficina de Transferencia de Conocimiento (OTC) Universidad Complutense de Madrid*.
- Jan Kietzmann et al, L. W. (2020). Deepfakes: Trick or treat? *ScienceDirect*.
- Jondec Briones, e. a. (2024). El uso ilícito de técnicas de inteligencia artificial y la necesidad de regulación: Deepfake. *Vniversitas*, 73.
- la Agência Nacional de Proteção de Dados (ANPD) . (2026). *ANPD publica Radar Tecnológico sobre deepfakes*.
- Palomo, R. (18 de 09 de 2023). Un año de libertad vigilada para 15 menores de Almendralejo por manipular imágenes de niñas. *El País*.
- Presidencia de la República de Colombia. (16 de mayo de 2022). Decreto 767 de 2022. Bogotá, Colombia.
- Presidencia de la República Federativa de Brasil. (14 de agosto de 2018). Ley 13.709 de 2018. Brasilia, Brasil.
- Presidencia de la República Federativa del Brasil. (10 de febrero de 2022). Enmienda Constitucional N° 115. Brasil.
- Rodríguez Pulecio, L. S. (2026). Deepfakes: la inteligencia artificial como nueva herramienta de violencia contra mujeres y niñas. *Agencia de Notificas Univalle*.
- Rodriguez, A. (13 de 10 de 2023). Acusado un universitario de alterar con inteligencia artificial miles de imágenes de alumnas para venderlas como pornografía. *El Pais Mexico* .
- Rodriguez, A. (23 de 05 de 2025). Sentenciado a cinco años de prisión Diego N, ex alumno del IPN, por el delito de pornografía infantil. *EL PAIS*.
- Sarraute Requeses, M. M., Avendaño Paredes, C. L., Torres Zambrano, Y., & Hidalgo López, R. (2025). *Fronteras Digitales y Violencia de Género: Un Estado del Arte en América Latina*. EDP University of Puerto Rico.
- Schwartz, O. (12 de 11 de 2018). You thought fake news was bad? Deep fakes are where truth goes to die. *The Guardian*. Obtenido de https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth?utm_source=chatgpt.com
- Serra, M. (29 de 06 de 2026). Paolla Oliveira relata su rutina con los abogados a causa de los deepfakes. *Nocitias ao Minuto Brasil*.
- SP2545-2020 , 52010 (Corte Suprema de Justicia, Sala Penal 22 de 07 de 2020).
- STP21973-2025, Radicación No. 150.278 (Sala Penal, Sala de decisión de tutela No. 2 Corte Suprema Justicia 02 de 12 de 2025).
- T-063/2024 (Corte Constitucional de Colombia 28 de febrero de 2024).
- T-090/1996 (Corte Constitucional de Colombia 06 de marzo de 1996).
- T-184/2026 (Corte Constitucional de Colombia 19 de junio de 2026).

T-280/2022 (Corte Constitucional de Colombia 8 de agosto de 2022).

T-289/2023 (Corte Constitucional de Colombia 2 de agosto de 2023).

T-339/2022 (Corte Constitucional de Colombia 28 de septiembre de 2022).

T-471/1999 (Corte Constitucional de Colombia 6 de julio de 1999).

T-561/2023 (Corte Constitucional de Colombia 15 de diciembre de 2023).

T-634/2013 (Corte Constitucional de Colombia 13 de septiembre de 2013).

Zago, B. (2025). Fraudes com deepfakes crescem 126% no Brasil em 2025. *BPMONEY*.