La responsabilidad civil extracontractual frente al uso de *DeepFakes*: posibilidad de una respuesta interpretativa desde el derecho colombiano vigente.

Determinación del régimen de imputación aplicable a los daños causados por el uso de *DeepFakes* en el marco de la responsabilidad civil extracontractual

Estefanía Ugarte Tapasco

Haein Jung

Monografía

UNIVERSIDAD EAFIT

Escuela de Derecho

Asesor: Esteban Mejía Rico

Medellín, Colombia

2025

Tabla de Contenido

Resumen

El *DeepFake* es una tecnología emergente que cuenta con un gran potencial para causar daños a derechos como la imagen, la honra o la intimidad, daños que podrían incluso materializarse en perjuicios patrimoniales. En Colombia no existe una regulación específica para este fenómeno en materia civil, lo que plantea un interrogante: ¿Bajo qué régimen de imputación podría establecerse responsabilidad civil extracontractual por los daños causados mediante el uso de *DeepFakes*? Esta monografía analiza el problema planteado considerando la solución que al mismo le han dado internacionalmente, e identificando los mecanismos de los que dispone el derecho colombiano para dicho propósito.

PALABRAS CLAVES

Responsabilidad civil extracontractual, *DeepFakes,* imputación objetiva, imputación subjetiva, inteligencia artificial, tratamiento de datos.

Abstract

DeepFake is an emerging technology that has great potential to cause harm to rights such as image, honor, or privacy, harms that could even materialize in economic damage. In Colombia there is no specific regulation addressing this phenomenon, which raises the following question: Under what liability regime could non-contractual civil liability be established for damages caused by the use of *Deepfakes*? This thesis examines the problem by considering the approaches adopted internationally and by identifying the mechanisms available under Colombia law for this purpose.

KEYWORDS

Extra-contractual Civil Liability, *DeepFakes*, Objective Imputation, Subjective Imputation, Artificial Intelligence, Data Processing.

1. Introducción.

Los *DeepFakes*, como videos, audios o imágenes falsificadas con inteligencia artificial, representan un nuevo desafío para los sistemas jurídicos. Estos contenidos podrían llegar a afectar gravemente derechos como la imagen, la honra, la intimidad y el buen nombre, e incluso causar daños patrimoniales. A pesar de lo anterior, Colombia no cuenta con una regulación específica para este fenómeno en materia civil, por lo que resulta necesario determinar si el régimen de responsabilidad civil extracontractual vigente cuenta con herramientas que nos permitan imputar responsabilidad por daños causados a través de esta tecnología, de manera eficaz y sin necesidad de una reforma legislativa.

Debido a que somos conscientes de la amplitud del problema planteado, nuestro estudio se centrará en establecer el régimen de imputación a través del cual podría atribuirse responsabilidad en casos de uso de *DeepFakes*. En este sentido, no entraremos a estudiar otros problemas que pueda representar dicho fenómeno, tales como, la causalidad, los retos en materia probatoria, o el trato que deba darse al mismo en otras áreas del derecho.

1.1 Justificación

En un contexto en que el desarrollo tecnológico es acelerado, este supera constantemente la capacidad regulatoria del derecho. Por lo anterior, resulta fundamental explorar alternativas que no impliquen reformas legislativas, pero que permitan dar una solución al problema; es decir, evaluar las herramientas con que cuenta el sistema, y establecer si a partir de las mismas podría llegarse a una solución efectiva frente al mismo.

El uso de *DeepFakes*, concretamente, plantea riesgos para diversos derechos protegidos por el ordenamiento, tanto de carácter patrimonial como extrapatrimonial: la honra, la imagen, el

buen nombre, entre otros. Lo anterior teniendo en cuenta que dicha tecnología puede resultar en contextos de violencia digital, fraude o suplantación.

El presente trabajo analiza cómo podría darse un trato adecuado, a través de la responsabilidad civil extracontractual, a los casos en los que se causan daños por el uso de *DeepFakes.* Puesto que el desarrollo legislativo y jurisprudencial en Colombia es prácticamente nulo, acudiremos a ejemplos de cómo otras jurisdicciones han abordado el tema. Al respecto, tomamos en consideración los sistemas jurídicos de Corea del Sur, Estados Unidos y Reino Unido, pues cuentan con un mayor desarrollo en este ámbito. Sin embargo, cabe aclarar que acudimos a ellos en un afán por encontrar referencias sobre el tema, pero entendemos que estas figuras no pueden simplemente transferirse al sistema colombiano, pues están diseñadas para contextos disímiles.

Teniendo en cuenta lo anterior, el abordaje del tema permite articular un análisis dogmático del derecho civil con un problema real y emergente; esto es, las tensiones que, de cara a derechos subjetivos, pueden traer consigo los avances tecnológicos. En este sentido, el presente trabajo es relevante para el estudio del Derecho en general, pues permite evidenciar la necesidad de que los juristas desarrollen una mirada crítica frente a la aplicación dinámica de las normas en contextos tecnológicos emergentes.

En el aspecto práctico, este tema también es de gran relevancia. La falta de un desarrollo jurídico trae consigo inseguridad jurídica. De un lado, de cara a los jueces, pues estos no cuentan con parámetros que les permitan decidir de manera uniforme a qué tipo de responsabilidad recurrir, lo que conlleva que pueda haber sentencias opuestas. De otro lado, en cuanto a las víctimas, la falta de regulación en materia de *DeepFakes* implica que estos no conozcan cómo abordar estos casos; esto es, a quién debe imputarse responsabilidad o qué debe probarse

concretamente en el proceso, lo que puede traer consigo que no se llegue a una reparación integral.

En estas circunstancias, es necesario dar respuesta al interrogante planteado. Debe tomarse conciencia sobre los peligros que puede representar la inteligencia artificial, concretamente los *DeepFakes*, y plantear mecanismos para contrarrestar los daños que se puedan ocasionar. Solo de esta forma se puede llegar a una interpretación uniforme de las leyes y brindar una protección efectiva a las víctimas, minimizando el vacío legal y fortaleciendo la confianza en la figura de la responsabilidad civil y el ordenamiento jurídico colombiano.

1.2 Objetivos Principales

Objetivo General

Analizar el régimen de responsabilidad civil extracontractual vigente en Colombia con el propósito de estudiar si, mediante una interpretación del mismo, es posible establecer el régimen de imputación a través del cual podría atribuirse responsabilidad en los casos en que se causen daños por el uso de *DeepFakes.*

Objetivos Específicos

- Describir el fenómeno de los *DeepFakes* desde sus características técnicas y riesgos jurídicos
- Estudiar las soluciones que internacionalmente se han dado a los casos de *DeepFake,* específicamente, las planteadas en el derecho estadounidense, europeo y surcoreano.
- Identificar la imputación como elemento de la responsabilidad civil y algunos de sus principales regímenes, de cara a la atribución de daños derivados de *Deepfakes.*
- Evaluar, frente a los daños generados por *DeepFakes,* la aplicabilidad de algunos regímenes de responsabilidad previstos en el ordenamiento jurídico colombiano.

- Proponer una alternativa interpretativa que permita aplicar el derecho vigente a los casos de uso de *DeepFakes.*

2. Marco Teórico

En este capítulo se presentan los fundamentos teóricos y dogmáticos que servirán de base para el análisis posterior de la imputación de responsabilidad en los casos de uso de *DeepFakes*. En primer lugar, se expone brevemente el régimen general de la responsabilidad civil extracontractual en Colombia, con sus elementos estructurales y modelos de imputación. Posteriormente, se introduce el fenómeno de los *DeepFakes*, con sus tipos y posibles riesgos. Lo anterior con el objetivo de construir el marco a partir del cual se desarrollará el presente trabajo.

2.1 La Responsabilidad Civil Extracontractual en Colombia.

La responsabilidad civil extracontractual se encuentra regulada en los artículos 2341 y siguientes del Código Civil Colombiano. De acuerdo con Trigo y López (2004) "responder civilmente, *latu sensu*, es el deber de resarcir los daños, ocasionados a otros, por una conducta lesiva antijurídica o contraria a derecho". En este sentido, la responsabilidad civil surgió como una alternativa a la venganza, que en las sociedades primitivas era el mecanismo predominante para reparar el daño, bajo el entendido de que se llegaba a la reparación infringiendo dolor al causante del daño (p. 19).

Dado lo anterior, de acuerdo con Trigo y López (2004) la responsabilidad civil busca cumplir 3 funciones: i) una función de reparación, en tanto dicha institución busca servir de medio jurídico para proporcionar una reparación a quien sufre un daño injusto; ii) una función demarcatoria, en tanto traza una frontera entre los casos en que los agentes pueden actuar libremente y aquellos en que sus conductas generan obligación resarcitoria; y iii) una función de

prevención del daño (pp. 60-61). Si bien en la doctrina aún se discuten otras funciones atribuibles a la responsabilidad civil, estas son las más aceptadas.

El ordenamiento colombiano distingue 2 tipos de responsabilidad civil. De un lado se encuentra la responsabilidad civil contractual, que podría definirse como aquella obligación indemnizatoria que deriva del incumplimiento de un contrato. De otro lado, se encuentra la responsabilidad civil extracontractual, que tiene lugar cuando se producen daños a terceros, pero la fuente del daño no es el incumplimiento de una obligación contractual[1]. En el presente trabajo nos centraremos únicamente en la responsabilidad extracontractual.

Adicionalmente, para que haya lugar a responsabilidad deben cumplirse ciertos elementos. De acuerdo con Flórez y Díaz (2022) del análisis sistemático del ordenamiento jurídico "se pueden enunciar hoy como presupuestos de la responsabilidad civil: el hecho generador imputable a un sujeto, el daño o perjuicio para otra persona (víctima) y la relación de causalidad entre el hecho imputable y el daño a la víctima" (p. 5). Sin embargo, dado el objetivo de la presente monografía, en este trabajo solo se ahondará en el elemento de la imputación.

2.1.1 De la Imputación: Regímenes Subjetivos y Objetivos

De acuerdo con Trigo y López (2004) para que surja responsabilidad, no basta la existencia de una conducta antijurídica, ni que se compruebe la relación causal, sino que adicionalmente se requiere que al acto generador del daño sea atribuible a una persona (p. 664). Al respecto, Baena (2021) señala que para que un hecho sea imputable es necesario que el mismo no se deba a una causa extraña o una causal de justificación. (p. 131)

[1] Según Tamayo (2007), "todo comportamiento ilícito que no se derive de la inejecución de un contrato válidamente celebrado entre demandante y demandado, genera responsabilidad civil extracontractual si se le ha causado daño a un tercero" (p. 575).

De acuerdo con Flórez y Díaz (2022), en cierto sentido, la categoría de "imputable" surge de la valoración de la culpa del agente. De allí la noción de "imputación subjetiva", que viene con el principio general de responsabilidad según el cual no puede atribuirse responsabilidad sin culpa (p. 10). Sin embargo, la evolución de la responsabilidad ha dado lugar a que no siempre sea necesario que el agente haya actuado culposa o dolosamente para que haya lugar a indemnizar.

Según Trigo y López (2004) en una perspectiva clásica, la culpa constituía un presupuesto esencial de la responsabilidad civil. Sin embargo, este enfoque estaba destinado mayormente a moralizar conductas individuales, pero no brindaba herramientas para reparar daños en un contexto tecnificado e industrializado en que se multiplicaban los riesgos (p. 24). Estos nuevos riesgos dieron lugar a la teoría del riesgo; esto es, doctrinas que, en forma parcial o total quieren prescindir del concepto de culpa y plantean supuesto de imputación objetiva[2].

De acuerdo con Tamayo (2007) "el artículo 2341 del Código Civil consagra el principio general de responsabilidad civil extracontractual. En esta norma se establece la responsabilidad delictual y cuasidelictual que se fundamenta en una culpa probada del autor del daño" (p. 35). En este sentido, este artículo contiene la regla general y la base de la imputación subjetiva, según la cual, no hay responsabilidad sin culpa[3].

No obstante, como se adelantó previamente, en el ordenamiento colombiano también se reconocen supuestos de responsabilidad objetiva; es decir, casos en que es posible atribuir

[2] Tamayo (2007) aclara que, no obstante, debe distinguirse entre la responsabilidad puramente objetiva y la responsabilidad objetiva por riesgo. La primera prescinde de cualquier elemento subjetivo; probando el vínculo causal entre el agente y el daño se produce la responsabilidad. En contraste, la teoría del riesgo prescinde de la idea de la culpa, pero acude al concepto de riesgo creado o riesgo-provecho. (p. 822)

[3] Flórez y Díaz. (2022) "a la "imputación subjetiva", que viene con el principio general de responsabilidad desde el código napoleónico y aparentemente superaba la simple iniuria objetiva: pas de responsabilité sans faute, no debía atribuirse responsabilidad sin culpa" (p. 6)

responsabilidad sin que sea necesario verificar un elemento de subjetivo como la culpa o dolo. Al respecto, en el presente trabajo se estudiarán algunos de estos regímenes especiales de imputación con el fin de dar luces sobre el régimen de imputación aplicable a los casos en que se cause daño por el uso de *DeepFakes*.

2.2. El Fenómeno *Deepfakes* como Objeto Jurídico

A continuación, se presenta una aproximación conceptual al fenómeno de los *DeepFakes,* con el fin de entender sus características técnicas, su impacto social y sus implicaciones jurídicas preliminares. Esta parte no busca aún imputar responsabilidades, sino describir el fenómeno como base fáctica para su análisis jurídico posterior.

2.2.1. Definición y clasificación técnica

El término *DeepFake* es la combinación de "*deep learning*" que en español traduce "aprendizaje profundo" y *"fake*" que significa falsificación. Se trata un tipo de inteligencia artificial (en adelante IA) que funciona a partir del entrenamiento y aprendizaje automático de dos modelos sobre una misma base de datos: un modelo generador, encargado de crear variables aleatorias a partir de una distribución predefinida, y un modelo discriminador que tiene como función determinar si los datos provienen del generador o del conjunto real. La interacción competitiva entre ambos modelos perfecciona las habilidades del generador, pues causa que las variables que este produzca se tornen indistinguibles para el discriminador (Rodrigo, 2021, p. 128).

Desde un punto de vista terminológico, Cambridge Dictionary lo define como "un video o grabación de sonido que reemplaza la cara o la voz de alguien con la de otra persona, de una manera que parece real" y, de forma similar, el Oxford English Dictionary lo describe como

> Cualquier contenido multimedia, especialmente videos, que ha sido manipulado digitalmente para sustituir de forma convincente la apariencia de una persona por la de otra, y que a menudo se emplea con fines maliciosos para mostrar a alguien realizando algo que en realidad no hizo.

Desde el punto de vista técnico y doctrinal, no existe una única definición universalmente usada del término *DeepFake*, pero existen ciertos elementos esenciales para su conceptualización. Según Spivak (2019), el término *DeepFake* se refiere a los videos en los que se insertan rostros hiperrealistas de una persona sobre el cuerpo de otra, con el propósito de crear una representación audiovisual falsa que simula ser auténtica (p. 339). Esta definición muestra la capacidad de alterar visualmente el rostro de otra persona, sin embargo, la definición no es suficiente por centrarse exclusivamente en la manipulación facial.

De forma más amplia, autores como Citron y Chesney (2019) definen los *DeepFakes* no solo como montajes pornográficos con rostros de celebridades, sino de forma más amplia; esto es, como toda falsificación digital hiperrealista de imágenes, audio o video. (p. 1757)

Por su parte, según Royer, Oerlemans y van Wegberg (2024), los *DeepFakes* son construcciones digitales producidas mediante algoritmos de aprendizaje profundo (*Deep learning*), que permiten reemplazar rostros o voces y generar contenidos audiovisuales nuevos (pp. 459-462). A partir de las definiciones anteriores, los *DeepFakes* constituyen una categoría especial de productos audiovisuales manipulados por las tecnologías avanzadas como lo es la inteligencia artificial.

Aunque las personas suelen asociar los *DeepFakes* necesariamente con prácticas ilícitas, esta idea no es correcta. Autores como Citron y Chesney (2019) han señalado que no toda la tecnología *DeepFake* es lesiva y que, en contraste, algunos usos de dicha tecnología resultan beneficiosos (p. 1968). Así mismo, en esta misma línea, dichos autores mencionan que “una prohibición general no es deseable porque la manipulación digital no es intrínsecamente

problemática. Los *DeepFakes* generan daños significativos en ciertos contextos, pero no en todos.” (p. 1788). Al respecto, señalan que algunos de los usos legítimos de los *DeepFake*s se encuentran en sectores como la educación, el arte, la salud, entre otros.

En primer lugar, en el ámbito educativo, estos permiten crear los contenidos interactivos que sean más atractivos para los estudiantes, ya sea utilizando simulaciones históricas o modificando escenas de películas con propósitos de enseñanza o científicos. Roh (2025), en su estudio constitucional sobre la expresión *DeepFake*, señala que estas tecnologías pueden emplearse para simular escenarios históricos o jurídicos que permiten al estudiante “interactuar con representaciones hiperrealistas de figuras del pasado o con testimonios virtuales”, lo cual potencia el aprendizaje. (pp. 84 - 88)

Por otro lado, el uso de esa tecnología en la cultura y el arte como cine, musicales y expresiones artísticas también ha sido muy común. En el ámbito cinematográfico, esta tecnología permite crear rostros de actores fallecidos, rejuvenecer a actores o incluso ayuda a crear un personaje nuevo con apariencia realista. Un ejemplo notable de esta idea se encuentra en *Killer Paradox* (Lee & Kim, 2024), una serie coreana en el cual el rostro de la infancia del actor principal fue recreado utilizando la tecnología *DeepFakes*, permitiendo una transición fluida entre escenas.

De manera similar, en la película *Top Gun: Maverick* (Kosinki, 2022), de Hollywood, a través del *DeepFakes* se recreó la voz del actor Val Kilmer, quien se encontraba afectado por un cáncer de garganta. Estas tecnologías no sólo ayudan a reducir el costo, sino que también abren nuevas posibilidades expresivas y artísticas.

Adicionalmente, esta herramienta también ha demostrado potencial en el sector de la salud. Al respecto, los *DeepFakes* se pueden usar para la rehabilitación comunicativa de

personas y también para la mejora de la precisión diagnóstica. Según Roh (2025), el instituto de informática Médica de la universidad de Lübeck de Alemania, desarrolló un sistema basado en *DeepFakes*, que permite generar imágenes médicas artificiales que simulan, con gran realismo, diferentes patologías (pp. 84 - 88). Así mismo, desde una perspectiva emocional, los *DeepFakes* también se han utilizado en procesos terapéuticos de duelo. En Corea, el programa de televisión "*I met you*" (MBC, 2020) recreó digitalmente a una niña fallecida para que su mamá pudiera despedirse de ella.

En el ámbito colombiano también hay un ejemplo significativo del uso de esta tecnología. Es el caso del político Rafael Pardo, primer ministro de Defensa civil del país, quien perdió la voz después de un accidente cerebrovascular en 2018. Gracias al uso de la tecnología *DeepFake* se pudo crear el pódcast "La Voz de Pardo" (Pardo, 2025) con la voz reconstruida.

2.2.2. Riesgos y daños jurídicamente relevantes

A pesar de sus aplicaciones legítimas, esta tecnología ha sido cuestionada por los daños causados a las víctimas cuando es usada con fines ilícitos o sin consentimiento. Los *DeepFakes* se han convertido en un instrumento de manipulación peligrosa. Existen varios usos ilícitos o ilegítimos de *DeepFakes* que causan daños a otros vulnerando los derechos de las víctimas.

Uno de los usos negativos más común de la tecnología *DeepFake* es la creación de vídeos de contenido sexual en los que se superpone el rostro de una persona real sobre cuerpos ajenos. Aunque estos videos de pornografía o fotos sexuales son contenidos falsos creados por IA, la precisión de esta tecnología hace cada vez más difícil distinguir lo real de lo falso. En palabras de Harris (2019):

> Hay un video tuyo teniendo relaciones sexuales en Internet. No recuerdas haber estado con esa persona porque nunca ocurrió. Otras personas también están viendo el video en línea. El video te resulta desconocido porque es un '*DeepFake*': un 'video falsificado ultra realista' en el que tu

> rostro ha sido superpuesto sobre el cuerpo de otra persona mediante el uso de software de inteligencia artificial (p.99).

Según Gieseke (2020), la pornografía *DeepFake* constituye una nueva forma de violencia sexual digital porque invade de manera persistente la privacidad y la autonomía de las víctimas (pp. 1482 - 1484). El problema más grande es que, una vez se viraliza, es casi imposible eliminar los videos en internet.

Además del daño individual que puede causar, el uso ilícito del *DeepFake* representa una amenaza creciente para la sociedad, pues puede afectar la estabilidad de los sistemas democráticos, la economía, la justicia, la seguridad internacional, entre otros. Citron y Chesney (2019) advierten que:

> El potencial de influir en el resultado de una elección es real, particularmente si el atacante logra distribuir el contenido en un momento tal que haya suficiente margen para que la falsificación se difunda, pero no el suficiente para que la víctima pueda desmentir de manera efectiva. (p. 1778)

En 2024, una investigación de *Security Hero* en los Estados Unidos reveló que más del 80% de los votantes creían que el contenido electoral producido por tecnología *DeepFakes* era auténtico. Más de un tercio de los encuestados dijo que la información que vieron los llevó a cambiar su intención de voto. Este estudio muestra que el impacto se acerca al 90% cuando los votantes están expuestos a videos manipulados donde sus candidatos preferidos promueven la violencia (como se citó en Roh, 2025, pp. 63 - 66).

Además del impacto político, el uso fraudulento de los *DeepFakes* ha comenzado a generar consecuencias en el ámbito económico y financiero. De acuerdo con Roh (2025), estos contenidos han sido utilizados para las estafas a través de videollamadas, simulaciones de voz, e incluso para vulnerar sistemas de seguridad bancaria (p. 63). Asimismo, Roh (2025) advierte que la reputación de una empresa puede verse afectada por falsos anuncios o reseñas de productos (p.

66). Al respecto, resulta relevante anotar que, en estos casos, no solo se pueden causar perjuicios morales por la afectación a bienes como la reputación, sino que estos pueden traducirse en consecuencias económicas como la pérdida de ingresos o la disminución del valor de las acciones.

Como se ha expuesto, los usos ilícitos de los *DeepFakes* representan riesgos para los derechos personalísimos y la dignidad humana. Lo que en apariencia puede parecer un simple montaje digital, se convierte, en muchos casos, en una agresión directa contra el honor, la intimidad, la imagen y el libre desarrollo de la personalidad. La gravedad del daño no depende de la veracidad del contenido, sino de su impacto social y subjetivo. Como lo ha reconocido Citron (2019), "los *DeepFakes* sexuales fuerzan a las personas a un sexo virtual, reduciéndolas a objetos sexuales" (p. 1921). Esta deshumanización viola principios constitucionales como la dignidad humana, la intimidad personal, reconocidos en los artículos 1 y 15 de la Constitución colombiana.

De hecho, aunque estos videos no contengan imágenes reales, su capacidad para invadir la esfera más íntima de una persona, los convierte en formas particulares de violencia simbólica. Como afirma Citron (2019) no representan cuerpos reales, pero secuestran la identidad sexual e íntima de las personas (p. 1921). Esta afirmación permite sostener que el daño inmaterial causado por los *DeepFakes* no depende de la existencia de una imagen auténtica, sino de la forma en que se instrumentaliza el cuerpo o la voz de otros para provocar humillación, vergüenza, angustia o aislamiento social.

Desde la perspectiva del daño moral, Royer et al. (2024,) advierten que las víctimas de este tipo de falsificaciones pueden sufrir trastornos severos como TEPT[4], ansiedad o ideación

[4] Trastorno de Estrés PosTraumático

suicida (pp. 467 - 468). A ello se suma la pérdida de confianza y control sobre la propia identidad, afectaciones que han sido reconocidas en la jurisprudencia colombiana como elementos suficientes para configurar responsabilidad extracontractual, incluso en ausencia de contacto físico o daño patrimonial directo.

En cuanto al daño patrimonial, el perjuicio también puede ser sustancial cuando la falsificación afecta la imagen pública de figuras reconocidas. De acuerdo con Spivak (2019), los *DeepFakes* pueden causar pérdidas económicas significativas a las personas afectadas, ya que su reputación, como un activo especialmente valioso, puede verse seriamente perjudicada, (p. 375). A esto se suma la dificultad práctica de ejercer mecanismos de defensa. Como señala Citron (2019), "sólo los casos extremos suelen captar la atención de las autoridades" (p. 1930). Esta falta de respuesta penal efectiva obliga a considerar seriamente la vía civil como herramienta principal de reparación, sobre todo cuando el contenido difundido vulnera derechos protegidos sin constituir un delito penal grave.

En definitiva, los *DeepFakes* representan, además de una amenaza tecnológica, una forma real de causar daño a las personas a través de la afectación a su imagen, su dignidad y su bienestar emocional. Aunque no siempre exista un contacto físico o un contenido verdadero, el impacto que generan es profundo y muchas veces duradero. Dado lo anterior, es necesario que el derecho civil reconozca estos daños y ofrezca mecanismos adecuados para proteger a las víctimas y reparar el daño causado. La respuesta jurídica no puede depender únicamente de si el contenido es real, sino de cómo afecta a los derechos de las personas en su vida cotidiana y entorno social.

3. Análisis de la Responsabilidad Civil Extracontractual Aplicada a los Daños Causados por el Uso de *Deepfakes.*

3.1 Análisis de Experiencias Internacionales:

El fenómeno de los *DeepFakes* se ha vuelto global y muchas jurisdicciones están evaluando ahora su infraestructura legal existente para adaptarla y abordar este problema. La tecnología es universal, pero las respuestas legales han asumido la forma específica de cada país, debido que cada sistema es "un legado de estas tradiciones legales y filosóficas previas" (Geng, 2023, p.162).

Para efectos comparativos y de referencia, el presente trabajo analiza los casos de Estados Unidos, la Unión Europea y Corea del Sur. Entre las razones para dicha selección, se encuentra que: (i) exhiben mayor dinamismo regulatorio y casos ya sometidos a control judicial; (ii) ofrecen modelos distintos para contrastar regímenes de imputación; y (iii) brindan lecciones que podrían tenerse en cuenta a la hora de establecer un tratamiento para el fenómeno de los *DeepFakes* en Colombia. A continuación, se explorarán sus enfoques.

3.1.1 Estados Unidos

La estrategia de EE. UU. para combatir el problema de los *DeepFakes* se representa como sectorial y desorganizada, gira en torno a iniciativas individuales de los estados sin una ley federal unificada respecto a esta amenaza. Esta fragmentación de la ley es un subproducto del sistema legal de EE. UU., en el cual las protecciones de la Primera Enmienda han dificultado la imposición de una regulación federal más general. (Geng, 2023, p, 162)

Geng (2023) advierte que los estados han tomado nota y han aprobado leyes en respuesta a estas preocupaciones. Por ejemplo, en 2019, California aprobó dos leyes que abordan diferentes aspectos de este problema: AB730 prohíbe el uso de *DeepFakes* políticos en un

contexto relacionado con campañas dentro de los sesenta días previos a una elección; y AB602 permite acciones civiles contra individuos y entidades que distribuyan *DeepFakes* de contenido sexual (p. 162).[5]

Además de California, Texas promulgó leyes que prohíben los *DeepFakes* relacionados con elecciones dentro de los últimos 30 días antes de una elección en 2019. Así mismo, Nueva York, desde 2023, ha criminalizado la distribución de ficción sexualmente explícita creada con IA sin el consentimiento de la víctima; y Dakota del Sur también reforzó su legislación en 2024 para imponer penas de cárcel por casos infantiles producidos por IA (Roh, 2025, pp. 138-154).

La tendencia actual de regulaciones en materia de *DeepFakes* ha sido influenciada significativamente por el caso Estados Unidos v. Alvarez (2012). En dicha oportunidad, la Corte Suprema dejó claro que "la falsedad por sí sola" no coloca una declaración fuera de la protección de la Primera Enmienda. El juez Kennedy escribió en su opinión que la falsedad en general merece protección, porque fomenta la refutación y "reaviva el respeto" por las ideas valiosas en el discurso público (Citron, 2019, pp. 1790-1791).

Sin embargo, todos los jueces estuvieron de acuerdo en que las declaraciones falsas que causen un "daño legalmente reconocible" pueden ser reguladas, aunque se dividieron sobre cómo podría ser tal regulación. Al respecto, tal jurisprudencia descarta, en gran parte, la idea de prohibir los *DeepFakes*, pero permite restricciones específicas diseñadas para los casos de difamación, fraude, amenazas verdaderas y la incitación inminente a la violencia; esto es, casos en los que los *DeepFakes* no son protegidos por el derecho a la libertad de expresión, previsto en la primera enmienda. (Citron, 2019, pp. 1790-1791)

[5] Tal como lo explica Geng (2023), California fue pionera en promulgar leyes enfocadas en *DeepFake*s, incluyendo la AB730 que prohíbe su uso dentro de los 60 días previos a una elección y faculta a los candidatos a solicitar medidas cautelares y la AB602 que crea una acción privada contra quienes difundan contenidos sexuales falsificados mediante *DeepFake*.

Sin un enfoque nacional uniforme, el Congreso, en los últimos años, ha llevado a cabo varios esfuerzos legislativos para intentar abordar el problema de diferentes maneras, estos incluyen:

- *No AI FRAUD Act* (2024), sobre los derechos de propiedad de las imágenes y la voz, que crea una acción civil para casos de uso o distribución no autorizados.
- *DeepFakes Accountability Act* (2023), para obligar a identificar y etiquetar contenidos manipulados a través de los *DeepFakes*.
- *DEFIANCE Act* (2024), que otorga derechos a aquellos que enfrentaron la creación sin acciones de consentimiento para demandar civilmente. (Roh, 2024, pp. 10-12)

Para febrero de 2024, el impulso estatal en las regulaciones se intensificó. Más de 40 estados introdujeron un total de 407 proyectos legislativos relacionados con la IA, muchos de ellos tocando el uso de los *DeepFakes*.

En cuanto al ejecutivo, en octubre de 2023, la Casa Blanca emitió la *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, abordando ocho principios para garantizar que esta tecnología, de rápida evolución, se utilice de manera responsable, desde proteger la privacidad, la seguridad y las libertades civiles hasta fomentar la transparencia y la responsabilidad. Cabe señalar que la orden ejecutiva no es un estándar legalmente vinculante sobre los *DeepFakes*, pero su agenda regulatoria adoptada anticipa un esfuerzo por controlar los usos ilegales de estas tecnologías. (Roh, 2024, p. 11)

En conclusión, Estados Unidos ha venido tratando el fenómeno de los *DeepFakes* a través de la combinación de varias figuras. Entre estas se destaca: i) el reconocimiento constitucional de la libertad de expresión con medidas estatales específicas; ii) proyectos de ley propuestos a nivel federal que están en trámite y iii) directivas administrativas. En este contexto,

es evidente que la estrategia estadounidense se ha centrado principalmente en emitir regulaciones adicionales, evitar una prohibición general de los *DeepFakes* y priorizar la protección del derecho a la libertad de expresión.

3.1.2 Europa

En Europa, la Unión Europea, UE, está adoptando un enfoque decididamente más integral, abordando los *DeepFakes* dentro de grandes marcos para la gobernanza de la IA. Este enfoque tiene más que ver con mitigar el riesgo que con prohibir la tecnología *DeepFakes* de manera centralizada. (Geng, 2023, p. 165)

Un ejemplo de lo anterior es el propuesto Reglamento de Inteligencia Artificial de la UE de 2021. Si bien esta norma no prohíbe los *DeepFakes*, reconoce que este tipo de tecnología es riesgosa, pues puede permitir la manipulación de información y, por tanto, señala que debe cumplir con los requisitos de transparencia previstos en el artículo 52 de dicho reglamento. En este contexto, es una tecnología que, en caso de utilizarse, se debe hacer la aclaración de que el contenido fue manipulado o generado por IA. Este método da primacía al derecho a la información precisa, intentando un delicado equilibrio entre la libertad de expresión y otros derechos básicos como la privacidad. (Geng, 2023, p. 166)

Siguiendo a Royer et al. (2024), además de la anterior, la UE ha implementado unas normas relevantes que se ocupan del problema. Esta estrategia se basa en dos normativas clave: Digital Service Ac (DSA)[6] que impone a los proveedores de servicios intermediarios obligaciones de diligencia debida respecto del contenido ilegal (p. 472). Lo anterior se entiende sin perjuicio de la criminalización de la difusión no consentida de material íntimo o manipulado, incorporada por la Directiva de la UE 2024/1385 sobre la lucha contra la violencia contra las

[6] La Ley de Servicios Digitales

mujeres y la violencia doméstica, que designa expresamente los *DeepFakes* como susceptible de causar un daño grave cuando imitan a una persona existente.

A partir de lo anterior, se observa que la UE ha buscado dar un trato más integral a la problemática, no hablando de prohibiciones, sino de métodos para mitigar los riesgos. Esta posición puede ser especialmente útil para establecer el tratamiento que, desde el derecho civil, se puede dar al *DeepFakes* en el contexto colombiano.

3.1.3 Corea del Sur

El entorno legislativo para los *DeepFakes* en Corea del Sur ha cambiado drásticamente. Ha pasado de unas pocas leyes anti-disrupción al establecimiento de un sistema de regulaciones mucho más robusto.

En un principio, apenas existía regulación sobre dicha materia, pero esta se limitaba a *DeepFakes* sexuales no consentidos. Entre ellas se encontraba la Ley de Promoción de la Utilización de Redes de Información y Comunicaciones y Protección de la Información, específicamente, su artículo 74. Sin embargo, dicha norma ofrecía un margen muy estrecho de aplicación de la persecución penal. Particularmente a raíz del caso Nth Room[7], se reveló que estas leyes eran anticuadas y no estaban a la altura.

Este movimiento llevó a Corea del Sur a cambiar su Ley sobre el Castigo de Delitos Sexuales en agosto de 2020, agregando el artículo 14-2 que criminaliza la creación de *DeepFakes* sexuales no consensuados (Roh, 2025, p. 112). Esa disposición convirtió en delito alterar, combinar o procesar imágenes para su distribución. Pero este estándar de intención de distribuir se convirtió en un obstáculo extremadamente alto para la persecución, permitiendo un

[7] Caso “Nth Room”: red de salas en Telegram (2018–2020) donde se coaccionó a mujeres y menores para producir y difundir material sexual; los autores recibieron condenas severas. El escándalo impulsó las “leyes anti-Nth Room”, incluyendo la tipificación específica de la fabricación y difusión de *DeepFakes* sexuales (art. 14-2).

vacío legal no intencionado, pues exigía demostrar la voluntad específica de difundir, lo que, en la práctica, dificultaba la persecución penal, incluso en casos evidentes.

La Ley sobre el Castigo de Delitos Sexuales fue revisada nuevamente en 2024, esta vez para llenar un vacío que se había vuelto cada vez más problemático. La enmienda eliminó del artículo 14-2 la frase "con el propósito de distribución", transformando así el mero hecho de que crear contenido manipulado es un delito, incluso si es solo para posesión personal. Esta reforma aumentó la duración de las penas de prisión y aplicó la criminalización para cubrir actos de posesión, compra, almacenamiento o visualización de material. Esta acción legislativa adoptó un enfoque mucho más activo y contundente, reconociendo que el acto de crear los *DeepFakes* no consensuados, en sí mismo, es absolutamente dañino. (Roh, 2025, p. 98)

Aunque la reforma legislativa se ha centrado en el ámbito penal, la vía civil en Corea del Sur no es residual, en contraste, se trata de un componente activo y persistente de la práctica judicial. Las víctimas ejercen activamente acciones de responsabilidad extracontractual con base en el artículo 750 de Código Civil, exigiendo indemnizaciones por daños morales y materiales causados por difamación, violación del derecho a la imagen o a la intimidad. Estas acciones generalmente se procesan de manera paralela o sucesiva a los procedimientos penales, aprovechando las condenas como pruebas contundentes de ilegalidad y causalidad. De esta manera, la regulación penal robusta y la utilización estratégica del marco civil existente han configurado una doble respuesta a la problemática que, a pesar de la ausencia de una norma exclusivamente civil sobre *DeepFakes*, es adecuada para la reparación de daños de la víctima.

3.2 Imputación de Responsabilidad Civil por Uso de Deepfakes en Colombia

A diferencia de los casos internacionales expuestos, en Colombia no ha habido mayor desarrollo del concepto de *DeepFakes*. La única mención hasta el momento, en materia

normativa, se dio a través del artículo 2 de la Ley 2502 del 28 de julio 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*". Allí se definió el término como "[...] la creación, modificación y utilización de un registro audiovisual, incluidas fotografías, videos, imágenes o grabaciones de sonido falsos, mediante Inteligencia artificial - IA - de manera que el registro parezca auténtico del discurso o conducta real de un individuo". Sin embargo, esta mención se hizo en el ámbito penal con el fin de introducir un agravante al delito de falsedad personal. Si bien probar la existencia de un delito facilita, en teoría, la consecución de una indemnización de perjuicios, hasta el momento no se han conocido casos en los cuales se analice civilmente la problemática de los *DeepFakes*.

A continuación, se expone cómo, a partir de las figuras de las que dispone el ordenamiento jurídico colombiano en materia de responsabilidad civil extracontractual, podría atribuirse responsabilidad por daños ocasionados por el empleo de *DeepFakes*. La presente sección empieza por referirse a la posibilidad de aplicar un régimen de responsabilidad subjetiva en el marco de daños causados por esta causa y termina analizando algunos regímenes especiales que podrían ser relevantes de cara al fin mencionado.

3.2.1 Imputación Subjetiva

3.2.1.1 De las Normas Relativas al Uso de la Imagen.

El derecho a la imagen ha sido abordado por diversas legislaciones bajo el entendido de que el mismo se asocia con la identidad personal[8], el buen nombre, la honra y la reputación. En el caso colombiano, el primer acercamiento a la idea de la imagen personal se dio la Ley 23 de

[8] Al respecto, Morales (2020) destaca que "en la actualidad, el concepto de imagen no se limita a la apariencia física de una persona, sino que se reputa de cualquier otro atributo que permita identificarla, como su voz, gestos, pelo, manera de vestir o de hablar, entre otros" (p. 9).

1982 "*Sobre derechos de autor*"[9] y posteriormente la Corte Constitucional lo reconoció como un derecho fundamental autónomo[10] vinculado con los derechos a la intimidad, honra y buen nombre. Así mismo, con la expedición de la Ley 1581 de 2012 se consideró la imagen como un dato personal de carácter biométrico y calificado como sensible (Morales, 2020, p.171).

> Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos[11]. (Art. 5, Ley 1581 de 2012.)

Así mismo, el artículo 6 de la Ley 1581 de 2012 refiere que el tratamiento de estos datos está prohibido salvo que 1) el titular lo haya autorizado (a menos que la Ley disponga que no se necesita autorización)[12]; 2) sea necesario el tratamiento para salvaguarda vital del titular y este se encuentre incapacitado física o jurídicamente (caso en que será necesaria la autorización de sus

---

[9] La Ley sobre derechos de autor prevé, en el artículo 36, que la publicación del retrato es libre si se relaciona con fines científicos, didácticos, culturales o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público. En contraste con los artículos 87 y 88 que dictan que las personas tienen derecho a impedir la exhibición de sus retratos si no hay consentimiento y que, cuando sea necesario el consentimiento de varias personas y haya desacuerdo, este debe ser resuelto por la autoridad competente.

[10] A este respecto, en la Sentencia T-405 del 24 de mayo de 2007, con el M.P. Jaime Córdoba Triviño se argumenta que: "El derecho a la imagen es sin embargo, un derecho autónomo que puede ser lesionado en forma independiente o concurrente con los derechos a la intimidad, a la honra y al buen nombre de su titular"

[11] De acuerdo con Morales (2020, p. 182), no hay una definición de "dato biométrico" en la legislación colombiana; sin embargo, el Reglamento General de Protección de Datos - RGDP (Reglamento (ue) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016) en su artículo 4º numeral 14 se indica que: "(…) 14) datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;". Asimismo, el numeral 51 de las consideraciones de este Reglamento establece que el tratamiento de fotografías no se considera en todos los casos tratamiento de datos biométricos, pues para que se considere tal, es necesario que estas permitan la identificación o la autenticación unívocas de una persona física.

[12] Como ejemplo de casos en que la Ley dispone que no se necesita autorización se cita el artículo 37 de la ley 23 de 1982, que dicta: "La publicación del retrato es libre cuando se relaciona con fines científicos, didácticos o culturales en general o con hechos o acontecimientos de interés público o que se hubieren desarrollado en público". Así mismo, el artículo 10 de la Ley 1581 dispone casos en que no es necesaria la autorización.

representantes legales; 3) se efectúe en el curso de actividades legítimas - y con las garantías correspondientes - por parte de organismos sin ánimo de lucro con finalidades políticas, filosóficas, religiosas o sindicales, siempre que se refiera a sus miembros o personas que mantengan contactos regulares por razón de su finalidad. En dicho evento, los datos no se podrán suministrar a terceros sin autorización del titular; 4) que el tratamiento sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial y; que el tratamiento tenga una finalidad histórica, estadística o científica. En estos eventos deben adoptarse las medidas conducentes a la supresión de identidad de los titulares.

Al respecto, se observa que la autorización es un eje central de la Ley 1581 del 2012. "De no existir consentimiento previo por el titular, los responsables o encargados del tratamiento de los datos no podrían recolectar ni mucho menos circular datos" (Aguilar, 2018, p. 26). Esta idea se refuerza con lo previsto en el artículo 9 de la Ley 1581 de 2012, según el cual *"*Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior".

Adicionalmente, la Ley 1581 de 2012 prevé, en el artículo 4 literal "d" el principio de veracidad o calidad. Este consiste en que "La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error". Al respecto, resulta necesario hacer referencia a la definición que la norma le otorga a "tratamiento", pues en esta se indica que es "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión".

3.2.1.2 De la culpa por contravenir lo establecido en la Ley de Protección de Datos Personales.

Como se explicó previamente, a través de los *DeepFakes,* es posible simular la identidad de otra persona, ya sea a través de imágenes, videos, o audios; lo que puede representar problemas de cara a las normas respecto del uso de la imagen personal. De acuerdo con Morales (2020), entre otros, algunos de los desafíos que esta tecnología representa son los siguientes: i) el interrogante sobre los requisitos que deberían cumplir los desarrolladores de IA para entrenar a las máquinas con cantidades abundantes de imágenes cumpliendo con la Ley 1581 de 2012 y; ii) la pregunta acerca de si, en estos casos, debe obtenerse autorización o se trata de fines científicos o culturales exentos del mencionado consentimiento (p. 191).

En esta oportunidad no entraremos a resolver los interrogantes en relación con si es necesaria o no la autorización en los casos de *DeepFakes* o si, por el contrario, se trataría de eventos en los que la Ley prevé expresamente que la autorización no es necesaria, como en el caso en que el uso de *DeepFakes* esté destinado a empleos culturales o científicos. No obstante, consideramos que es necesario tener presente estos interrogantes, pues según el uso que se le dé a esta, dependerá si se requiere o no el deber de obtener una autorización para el tratamiento de datos, lo cual conduciría a aplicar o no un régimen subjetivo de responsabilidad.

Respecto del elemento subjetivo, vale decir que cuando hablamos de "culpa" nos referimos a una conducta negligente o a una falta, en este sentido, podemos hablar de culpa a título de dolo o de culpa en sentido estricto (Tamayo, 2007, p. 192). Bajo esta concepción, se identifican dos supuestos en los que podría haber lugar a culpa de acuerdo con lo establecido en la Ley 1581 de 2012.

En primer lugar, tenemos que se podría configurar culpa cuando se contraría la prohibición de tratamiento de datos personales sin autorización. Sin embargo, esto sólo sería posible si entendiéramos que en los casos de *DeepFakes* es igualmente aplicable la prohibición presente en la Ley 1581 de 2012 respecto del tratamiento de datos sin autorización[13].

En segundo lugar, el otro supuesto de culpa se presentaría al argumentar que se contradijo el principio de veracidad y calidad. Esta falta es más o menos fácil de demostrar si se tiene en cuenta que precisamente los *DeepFakes* permiten crear falsificaciones hiperrealistas de imágenes, videos y audios (Citron y Chesney, 2019, p. 1757). No obstante, consideramos que el uso de *DeepFakes* no implica necesariamente contradecir este principio, pues el hecho de aclarar, por ejemplo, que se trata de *DeepFakes*, implicaría que no se está realmente induciendo al error[14].

A pesar de lo anterior; esto es, que podría configurarse culpa por contradecir lo indicado en la Ley 1581 de 2012, el régimen subjetivo no parece brindar una solución satisfactoria a la pregunta sobre la imputación en los casos de los daños ocasionados por *DeepFakes*. Incluso si se toma la posición según la cual el régimen aplicable sería el subjetivo por tratarse de un tratamiento no autorizado de datos o al contradecir el principio de veracidad y calidad, este régimen parece no ser suficiente.

Por su parte, en el ámbito de la inteligencia artificial hay varios agentes implicados: la empresa que ostenta los derechos sobre el software, los desarrolladores y los usuarios; de lo cual se infiere que no resulta claro a cuál de ellos le sería imputable la conducta culposa (Ortiz

[13] De acuerdo con Morales (2020) este es uno de los interrogantes que deben ser resueltos de cara al tratamiento de los datos cuando estos son tratados a partir de inteligencia artificial generativa (p. 191).

[14]Hacemos esta afirmación refiriéndonos únicamente al cumplimiento o no del principio, pues al analizar la responsabilidad civil la mera producción de *DeepFakes* tendría una incidencia causal importante en el daño.

Figueroa, Ortiz Flórez, 2024, párr. 5)[15]. Esta indeterminación resulta problemática, pues la imputación de responsabilidad exige, en principio, identificar al sujeto responsable.

Además, esta determinación se hace más problemática dada la definición que atribuye la misma Ley 1581 de 2012, en su artículo 3, al término "tratamiento", pues en ella se incluyen verbos como: "recolección, almacenamiento, uso, circulación o supresión". Lo anterior implica que tanto la empresa que ostenta los derechos sobre el software como los desarrolladores y los usuarios podrían estar tratando datos según la misma definición.

Por su parte, la jurisprudencia ha previsto figuras como la culpa organizacional para no tener que establecerla en un solo sujeto y, en contraste, habla más bien de la culpa de la organización:

> Cierto es que los sistemas organizativos sólo pueden tomar decisiones y actuar a través de los seres humanos que los conforman, pero de ahí a dar por sentado que sólo son imputables las personas naturales hay una enorme distancia. Una cosa es que los procesos organizacionales con aptitud de ocasionar daños a terceros necesiten de la intervención humana para su realización, y otra bien distinta que esos procesos sólo sean atribuibles a los miembros de la organización en tanto individuos de la especie humana (Corte Suprema de Justicia, Sentencia del 30 de septiembre de 2016).

No obstante, la Corte ha reconocido esta posibilidad en el ámbito de las personas jurídicas. Si bien algunos autores han señalado que esta figura podría ser de utilidad cuando se trata de robots autónomos (Flórez y Díaz, 2022, p. 26), esta posibilidad no parece ser aplicable a los casos de *DeepFakes*, pues en ellos no existe un robot autónomo, sino que es la tecnología quien responde a lo que le soliciten los usuarios. En este contexto, consideramos que no sería

[15]Así mismo, estos autores se plantean el interrogante de si, en estos casos, la omisión de los programadores y las empresas de IA al momento de establecer límites, prohibiciones e instrucciones de buen uso para los usuarios podría constituir el hecho generador del daño.

posible hacer una analogía entre este tipo de inteligencia artificial y las personas jurídicas. Por lo tanto, la culpa organizacional no ofrecería una respuesta satisfactoria al problema sobre a quién imputar la responsabilidad.

De acuerdo con lo anterior y con las herramientas de las que el ordenamiento jurídico colombiano dispone, consideramos que podría llegarse a una solución teniendo en cuenta dos alternativas. De un lado, a través del análisis del elemento de la causalidad[16], según el cual puede establecerse el agente que tiene mayor incidencia en la causación del resultado y, por lo tanto, sentar las bases para establecer a cuál de ellos se le atribuye el daño[17]. No obstante, dado que el objetivo del presente trabajo es tratar el elemento de la imputación, no entraremos a detallar este asunto.

De otro lado, sería posible seguir la línea que el legislador fijó a través de la Ley 2502 del 28 de julio 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 se dictan otras disposiciones*". Al respecto, esta Ley modificó el artículo 296 al establecer que:

> El que con el fin de obtener un provecho para sí o para otro, o causar daño, sustituya o suplante a una persona o se atribuya nombre, edad, estado civil, o calidad que pueda tener efectos jurídicos, incurrirá en multa, siempre que la conducta no constituya otro delito.

[16] De acuerdo con Ortiz Figueroa y Ortiz Flórez (2024) para establecer cómo opera la imputación y el análisis de culpa en estos casos " [...] es fundamental acudir a la teoría de la causalidad adecuada (a través de la cual se supera la teoría de la equivalencia de las condiciones), para hacer un análisis completo sobre el nexo causal para cada caso en específico y, de esta forma, determinar a cuál de todas las partes involucradas le es realmente atribuible el daño ocasionado, entendiendo que, si bien todos estos sujetos participan y sus conductas pueden ser condición del daño, no son necesariamente su causa." (párrafo 8)

[17] De acuerdo con Rojas y Mojica (2014) "En Colombia, la jurisprudencia de la Corte Suprema de Justicia en su Sala de Casación Civil ha acogido la teoría de la causalidad adecuada como herramienta para señalar cuándo una actuación ha sido la causa de un daño y, a partir de ello, condenar a su autor a reparar el perjuicio irrogado" (p. 194)

Cuando la falsedad personal se realizare con la utilización de Inteligencia Artificial la multa se aumentará hasta en una tercera parte, siempre que la conducta no constituya otro delito. (El resaltado es nuestro)

A partir de lo anterior, podríamos decir que, en el ámbito penal, la conducta típica se atribuye al sujeto que busque causar daño o sacar provecho de la suplantación de identidad. En este sentido, se atribuye responsabilidad penal al usuario de la IA, no a los programadores ni a quienes ostentan los derechos sobre el software. Sin embargo, resulta claro que la responsabilidad civil y la penal persiguen fines distintos y poseen figuras distintas, de ahí que no parezca adecuado aplicar descuidadamente una analogía[18].

En conclusión, la aplicación de un régimen de imputación subjetiva a los casos de *DeepFakes,* aunque puede ser viable, presenta ciertas limitaciones. Es posible sostener que se configure culpa cuando se contraría la prohibición de tratamiento de datos personales sin autorización o el principio de veracidad y calidad consagrado en la Ley 1582 de 2012. No obstante, es complicado establecer a quién debe imputarse responsabilidad en estos casos; esto es, si el deber de cuidado recae sobre los programadores, las empresas que ostentan los derechos sobre el *software* o los usuarios. Sin embargo, consideramos que este interrogante podría resolverse a través de un análisis de la causalidad. En este sentido, si bien la aplicación de este régimen presenta limitaciones, podría resultar viable.

3.2.2 Regímenes especiales de imputación

[18] A este respecto, Trigo y López (2004) plantean lo siguiente: "la exculpación del autor o participe en sede penal no es óbice para que responda civilmente; es un principio asentado en nuestro derecho que con los mismos elementos de prueba, se puede absolver al demandado por no haberse comprobado responsabilidad penal en un accidente de tránsito y adoptarse una decisión inversa en orden a la responsabilidad civil del mismo, ya que la responsabilidad penal y civil no se confunden, porque se aprecian con criterio distinto y por consiguiente puede afirmarse la segunda aunque se haya establecido la inexistencia de la primera" (p. 12).

A continuación, se abordarán algunos tipos de responsabilidad civil extracontractual que contemplan regímenes de imputación que podrían considerarse "especiales", en la medida en que se apartan del enfoque tradicional; esto es, no exigen la verificación de la culpa como elemento constitutivo de responsabilidad civil u operan bajo la presunción de esta[19]. El propósito del análisis es estudiar la posible aplicabilidad de estas figuras en los casos de daños causados por *DeepFakes*.

3.2.2.1 Responsabilidad por el ejercicio de actividades peligrosas.

El Código Civil Colombiano en el artículo 2356 prevé un caso especial frente al régimen de responsabilidad con culpa (Velásquez, 2009, p. 516). Esta disposición dicta lo siguiente:

> Por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona debe ser reparado por ésta.
>
> Son especialmente obligados a esta reparación:
>
> 1. El que dispara imprudentemente un arma de fuego.
>
> 2. El que remueve las losas de una acequia o cañería, o las descubre en calle o camino, sin las precauciones necesarias para que no caigan los que por allí transiten de día o de noche.
>
> 3. El que esté obligado a la construcción o reparación de un acueducto o fuente, que atraviesa un camino, lo tiene en estado de causar daño a los que transitan por el camino.

Si bien la disposición transcrita empieza por señalar que el daño debe poder imputarse a dolo o culpa, a continuación, se establece que en ciertas hipótesis hay una obligación especial de reparación (Velásquez, 2009, p. 516). Esta precisión llevó a que la doctrina y la jurisprudencia interpretaran que se trataba de un régimen distinto al previsto en el artículo 2341 del Código Civil. Para Montoya Gómez el artículo 2356 del Código Civil "consagra una presunción de culpa, la que se presume de derecho, a cargo de quien al ejercer una actividad peligrosa lesione

[19] Se habla de presunción de culpa porque la víctima no tiene la carga de probar la culpa del demandado.

un derecho ajeno[20]. El demandado en este caso sólo puede eximirse de responsabilidad demostrando el elemento extraño" (como se citó en Tamayo, 2007, p. 869). En la práctica, puesto que el demandado sólo puede eximirse de responsabilidad probando causa extraña, esta figura es equiparable a un tipo de responsabilidad sin culpa (Tamayo, 2007, p. 869.).

Teniendo claro en qué consiste el régimen, es importante señalar que el responsable en el mismo es quien tiene la guarda material de la actividad. Según Cárdenas y Gómez (2020) en el régimen de responsabilidad por actividades peligrosas esta se atribuye al guardián de la misma, pues se entiende que es el responsable de ella y de los daños que pueda ocasionar.

> Por guardián se entiende aquel que tiene el poder intelectual de dirección y control sobre la cosa a través de la cual se ejerce la actividad peligrosa, el cual puede encontrarse en cabeza de diferentes personas desde diferentes relaciones de hecho (p. 85).

En Colombia, si bien está claro que actualmente existe esta forma de responsabilidad en el ordenamiento jurídico, persisten dudas sobre su naturaleza exacta; esto es, no resulta claro si la misma adopta una teoría de riesgo en su sentido más puro; es decir, un régimen de responsabilidad objetiva o sin culpa o, por el contrario, adoptó un régimen en el cual se presume la culpa (Velasquez, 2009, pp. 517-518). En la jurisprudencia colombiana si bien en la mayoría de los casos se ha señalado que se trata de un régimen de culpa presunta[21], en algunos casos se ha señalado que, en realidad, se trata de un régimen objetivo o sin culpa[22].

---

[20] Tamayo (2007) define la actividad peligrosa como "toda actividad que, una vez desplegada, su estructura o su comportamiento generan más probabilidades de daño de las que normalmente está en capacidad de soportar por sí solo un hombre común y corriente. Esta peligrosidad surge porque los efectos de la actividad se vuelven incontrolables o imprevisibles debido a la multiplicación de energía y movimiento, a la incertidumbre de los efectos del fenómeno o a la capacidad de destrozo que tienen sus elementos". (p. 935)

[21] En Sentencia del 9 de septiembre de 1948 la Corte Suprema de Justicia indicó: "la interpretación que se ha de dar al artículo 2356 del Código civil no equivale ni con mucho a la admisión de la teoría del riesgo, acerca de la cual ha puesto de presente nuestra sala que nuestras leyes no la acogen".

[22] La Sentencia SC 2111 de 2021 establece: "De tal modo que la responsabilidad por actividades peligrosas no se ancla a un tipo de responsabilidad subjetiva [...] realmente se enmarca en un sistema objetivo, porque en ninguna de tales hipótesis el agente se exime probando diligencia y cuidado, sino cuando demuestra causa extraña.

Responsabilidad Civil por el Ejercicio de Actividades Peligrosas Aplicada a los Daños Causados por Deepfakes.

Dado que el presupuesto para que este régimen sea aplicable es la presencia de una actividad peligrosa[23], es necesario establecer si el uso de *DeepFakes* puede catalogarse como tal. De acuerdo con Jiménez (2025) para dicho propósito es necesario identificar la clase y el nivel de riesgo del sistema de IA que estamos estudiando. La IA podría considerarse como una actividad peligrosa si crea un riesgo excepcional para las personas o bienes, que no puede disminuirse o eliminarse mediante un actuar diligente (p. 205). A este respecto de las actividades peligrosas, la jurisprudencia colombiana ha señalado que:

> Aunque el Código Civil Colombiano, no define la "actividad peligrosa", ni fija pautas para su regulación, la Corte ha tenido oportunidad de precisar que, por tal, debe entenderse aquélla que "…aunque **lícita,** es de las que **implican riesgos de tal naturaleza que hacen inminente la ocurrencia de daños**,…"(G.J. CXLII, pág. 173, reiterada en la CCXVI, pág. 504), o la que "… debido a la manipulación de ciertas cosas o al ejercicio de una conducta específica que **lleva insito el riesgo de producir una lesión o menoscabo**, tiene la **aptitud de provocar un desequilibrio** o alteración en las fuerzas que –de ordinario- despliega una persona respecto de otra[24]

En síntesis, la Corte ha establecido que para que una actividad sea considerada peligrosa esta debe ser 1) lícita; 2) implicar riesgos que hagan inminente la ocurrencia de daños y; 3)

---

[23] "a la víctima le basta acreditar el ejercicio de la actividad peligrosa desarrollada por su contendiente, el daño que padeció y la relación de causalidad entre aquella y este; al paso que el demandado sólo puede exonerarse demostrando que el perjuicio no fue producido por dicha operación, es decir, que obedeció al devenir de un elemento extraño y exclusivo, como la fuerza mayor o caso fortuito, la intervención de la víctima o la de un tercero, únicas circunstancias que rompen el nexo causal citado» (CSJ SC2905-2021 de 29 de jul. Rad. 2015-00230-01)

[24] Así lo señaló la Corte Suprema de Justicia en la Sentencia del 26 de agosto de dos mil diez (2010) con M.P RUTH MARINA DÍAZ RUEDA (Rad. 4700131030032005-00611) en la que reiteró lo expuesto en la sentencia de octubre 23 de 2001, expediente 6315.

provocar un desequilibrio. A continuación, se expone por qué, de acuerdo con estos elementos, la creación de *DeepFakes* podría constituirse como tal en una actividad peligrosa.

En primer lugar, en relación con la licitud, la generación de *DeepFakes* no es una actividad ilícita en abstracto. Si bien, como se explicó previamente, es posible que se dé un uso ilícito a esta tecnología; esto es, si se contradice la prohibición de tratar datos personales sin autorización, el principio de veracidad y calidad o incluso si se incurre en un delito a través de ella, en Colombia no existe una prohibición general para dicha actividad.

Adicionalmente, resulta útil recalcar que la Corte Suprema de Justicia ha indicado que, si bien las actividades peligrosas son por lo general lícitas; esto es, admitidas y permitidas por el ordenamiento jurídico, es factible el ejercicio ilícito de una actividad de esta naturaleza, lo cual no excluye la aplicación del régimen de responsabilidad por actividades peligrosas, pues este no se sustenta en la licitud de la conducta, sino en el riesgo potencial de lesión a intereses protegidos (Corte Suprema de Justicia, sentencia del 18 de septiembre de 2009).

En segundo lugar, respecto del elemento según el cual una actividad peligrosa debe implicar riesgos que hagan inminente la ocurrencia de daños, Jiménez (2025) señala que el nivel de riesgo de una IA puede variar por distintos factores "[...] como si manejan datos sensibles de las personas o toman decisiones sin supervisión humana en áreas de interés general como lo es la salud" (p. 203). En este sentido, podríamos decir que, dado que los *DeepFakes* pueden manipular datos sensibles y permiten fácilmente suplantar la identidad de las personas, estos conducen a riesgos que hacen inminente la afectación a bienes jurídicos como el buen nombre[25].

No obstante, vale la pena recalcar lo que la jurisprudencia colombiana ha entendido por actividades inminentemente peligrosas, pues estas se han relacionado tradicionalmente con la

[25] De acuerdo con la definición de Tamayo (2007) podría afirmarse que es un caso de peligrosidad en el comportamiento, pues del uso que se dé a esta tecnología, la misma puede derivar en una actividad peligrosa (p. 941)

multiplicación de energía y movimiento. Al respecto, la Corte Suprema de Justicia en la sentencia SC4204-2021, Radicación n.° 05001-31-03-003-2004-00273-02, reiteró la Sentencia SC002 del 12 de enero de 2018, Rad. n.° 2010-00578-01 y señaló que el concepto de actividad peligrosa:

> *[...] no ha sido definido bajo un criterio jurídico general, sino que suele explicarse mediante ejemplos tales como la velocidad alcanzada, la naturaleza explosiva o inflamable de la cosa utilizada, la energía desplegada o conducida, entre otras situaciones cuya caracterización ha sido delimitada por la jurisprudencia*.

Visto lo anterior, no parece del todo acorde con la jurisprudencia actual otorgar la categoría de actividad peligrosa a la generación de *DeepFakes*. Sin embargo, en algunos pronunciamientos se ha acogido la posibilidad de que ciertas actividades, aún sin cumplir con las características tradicionales de lo peligroso, puedan considerarse riesgosas[26]. Un ejemplo de lo anterior se da en el ámbito de responsabilidad bancaria. En estos casos, aunque no se ha acogido un régimen de responsabilidad por actividades peligrosas, sí se ha señalado que se trata de una actividad riesgosa[27].

Ahora bien, las razones por las cuales la jurisprudencia le ha dado la connotación de riesgosa, en lugar de peligrosa, a la actividad bancaria son dos: en primer lugar, porque la responsabilidad bancaria es de tipo contractual, por lo que el fundamento normativo es distinto.

---

[26] Al respecto, es importante recalcar que la Corte Suprema de Justicia en la Sentencia SC4204-2021 estableció que "si bien toda actividad peligrosa es riesgosa, no toda actividad riesgosa es peligrosa. Riesgo y peligro, conceptual y fenomenológicamente presentan diferencias. [...] por peligro se entiende el riesgo o contingencia inminente de que suceda algún mal; y por riesgo, la contingencia o proximidad de un daño

[27] "[...] el ordenamiento reclama que el ejercicio de la actividad bancaria atienda rigurosos parámetros de capital, apalancamiento, liquidez, gobierno corporativo, riesgo de crédito y composición patrimonial, por citar algunas variables [...] Estas imposiciones legales y reglamentarias, proporcionales a los enormes riesgos morales, operativos, de crédito, de seguridad, entre otros, que son connaturales al giro de los negocios bancarios, muestran que las entidades financieras asumen con la sociedad un compromiso de evitación de esas amenazas, de modo que serán aquellas quienes deban responder si estas se materializan, sin ninguna consideración adicional." (Corte Suprema de Justicia en la Sentencia SC4204-2021)

En segundo lugar, porque una parte de la jurisprudencia entiende que el artículo 2356 consagra un régimen subjetivo de responsabilidad, lo que sería incompatible con la responsabilidad por riesgo (Corte Suprema de Justicia, SC4204-2021). De este modo, si la negativa a aplicar un régimen de responsabilidad por actividades peligrosas para la actividad bancaria obedece a consideraciones diferentes a su posible carácter peligroso, cabría pensar que esta connotación pueda darse a actividades que, sin implicar fuerza o velocidad generen peligros relevantes, como lo sería la creación de *DeepFakes*.

Siguiendo la línea anterior, consideramos que los riesgos que representa la generación de *DeepFakes* no pueden eliminarse a través del actuar diligente. Por un lado, la empresa o los programadores, si bien pueden establecer, por ejemplo, instrucciones de uso, estos no pueden controlar realmente que los usuarios sigan o no dichos parámetros. En este mismo sentido, si bien los usuarios pueden aclarar que se trata de imágenes, videos o audios generados con IA, esto no impide, por ejemplo, que terceros los divulguen y con ello se generen perjuicios[28]. Dado lo anterior, algunos autores proponen responsabilizar a las plataformas ante los casos de *DeepFakes* con fines delictivos[29].

En este punto resulta útil traer a colación lo propuesto en el Reglamento de Inteligencia Artificial de la UE de 2021, en donde también se reconoce el riesgo que conllevan los *DeepFakes*. Allí, como se explicó previamente, se establece que los *DeepFakes* son tecnologías que conllevan riesgos de manipulación y, en respuesta a esta situación, se establece la obligación

[28] En este aspecto consideramos que difícilmente puede acudirse al hecho de un tercero como causal eximente de responsabilidad pues, de acuerdo con la jurisprudencia, para aludir a dicha causal el hecho debe ostentar las características de ser imprevisible e irresistible para el eventual responsable, de suerte que se genere la "ruptura" de la relación causal, cuya eficacia pende del hecho de que tal «conducta sea la única causa de la lesión, "en cuyo caso, a más de exclusiva, eficaz, decisiva, definitiva e idónea del quebranto, es menester "que el hecho fuente del perjuicio no haya podido ser previsto o evitado por el demandado" (SC065-2023 M.P Hilda Gonzales Neira)

[29] Así lo propone Rodrigo López (2021, p. 140) "Following the Chinese regulators' approach of making social media companies accountable for the creation and propagation of *DeepFakes* could be an effective way to deter the use of *DeepFakes* for criminal purposes, as *DeepFakes* go viral on social networks "

de advertir cuando la información haya sido alterada o generada por IA. Si bien esta norma no es aplicable a Colombia, consideramos que acciones como aclarar el origen de la información pueden ser exigibles en el contexto colombiano, en tanto, de acuerdo con la constitución, el derecho a la libertad de expresión implica diligencia[30].

Por último, en cuanto al elemento según el cual una actividad peligrosa debe producir un desequilibrio o alteración en las fuerzas que de ordinario despliega una persona respecto de otra, consideramos que también se cumple. El *DeepFake* es una tecnología que facilita la suplantación de identidad al crear objetos hiperrealistas que pueden confundirse con la realidad, de ahí pueda ponerse en una situación de indefensión a la víctima. A esta le resulta muy complicado probar que dicha información no es verídica.

No obstante, en este punto, de nuevo no resulta tan sencillo encajar la idea en lo que la jurisprudencia colombiana ha entendido por desequilibrio. La jurisprudencia ha señalado que este término se refiere a fuerzas físicas, a los casos en que un sujeto adiciona a su energía otra extraña y por esto pone en peligro a terceros (CSJ, Exp. 7623, 2024). En consecuencia, la generación de *DeepFakes* tampoco parece ajustarse al requisito de producir un desequilibrio. Sin embargo, aquí nuevamente es útil remitirnos a pronunciamientos sobre responsabilidad bancaria, pues en ellos se ha planteado otra forma de ver el desequilibrio:

> El cuentahabiente no custodia el dinero depositado, ni participa de las decisiones operativas del banco. Además, no tiene acceso a la información necesaria para afrontar peligros como los anotados, ni le resulta económicamente razonable hacerlo, pues los costos de esa faena serán, casi invariablemente, superiores a la pérdida que pretende prevenir; en cambio, para el banco la

[30] A este respecto, es importante tener en cuenta lo dictado por la Corte Constitucional en la Sentencia T243/18, con M.P Diana Fajardo Rivera, según la cual "[...] de la libertad de expresión se exige que diferencie hechos de opiniones, y en la medida en que incluya supuestos fácticos equivocados o falsos, puede ser sometida a rectificación. [...] Con todo, ambas libertades deben ejercerse responsablemente, pues no pueden irrespetar los derechos de los demás."

> situación es exactamente la opuesta, lo que justifica que sea él quien asuma el riesgo de su operación, de manera objetiva. (CSJ SC5176-2020, Radicación n.° 11001-31-03-028-2006-00466-01).

En este sentido, la sentencia citada sugiere que el desequilibrio podría entenderse como un desnivel en las capacidades para afrontar los peligros. Si bien, como se explicó previamente, la Corte ha sostenido que la actividad bancaria no puede regirse bajo el modelo de responsabilidad por actividades peligrosas, sí establece que, en tales casos, las partes no se encuentran en igualdad de condiciones para actuar, por lo que quien debería asumir el peligro es quien se encuentra en mejores condiciones para hacerlo[31]. A la luz de este precedente, podría entenderse que en la generación de *DeepFakes* también se presenta un desequilibrio entre quien produce el *DeepFake* y la víctima.

Una vez comprobado que la creación de *DeepFakes* podría constituir una actividad peligrosa, es importante hacer dos aclaraciones. De un lado, cabe precisar que las actividades peligrosas no solo atienden a estos criterios, sino que puede haber otras razones por las cuales las mismas no se consideren tales[32]. Por otro lado, si bien parece que podría aplicarse el régimen de

---

[31] "El régimen de responsabilidad de los Bancos por la defraudación con el uso de instrumentos espurios para disponer de los fondos depositados en cuentas, se ha fundado en vertientes de la teoría del riesgo: En una primera época, la del "riesgo creado" en virtud de la cual quien en desarrollo de una actividad genere un peligro o contingencia, debe indemnizar los perjuicios que de aquel deriven para terceros, con independencia de si ha actuado de manera diligente o culposa, o de si ha obtenido o un provecho; después se dio aplicación a la teoría del "riesgo provecho" que carga con la obligación resarcitoria a quien ejerza la actividad que genera un riesgo o peligro y, además, saca de la misma una utilidad o percibe lucro, sin que importe que su conducta haya sido diligente o imprudente; por último, se acudió a la teoría del "riesgo profesional" que es una derivación de la anterior, empleada también en otras áreas del derecho como, por ejemplo, en materia de accidentes y enfermedades laborales. En esta última, la obligación de asumir los riesgos inherentes al ejercicio de la actividad se basa en el profesionalismo que esta requiere" (CSJ SC18614-2016, citada en la SC5176-2020).

[32] Es el caso de la actividad médica, que no ha sido considerada peligrosa, entre otras razones, debido a los fundamentos que la justifican. En la sentencia de 30 de enero de 2001, expediente No. 5507, la Corte Suprema de justicia señaló que: "Ciertamente, el acto médico y quirúrgico muchas veces comporta un riesgo, pero éste, al contrario de lo que sucede con la mayoría de las conductas que la jurisprudencia ha signado como actividades peligrosas en consideración al potencial riesgo que generan y al estado de indefensión en que se colocan los asociados, tiene fundamentos éticos, científicos y de solidaridad que lo justifican y lo proponen ontológica y razonablemente necesario para el bienestar del paciente, y si se quiere legalmente imperativo para quien ha sido capacitado como profesional de la medicina, no sólo por el principio de solidaridad social que como deber ciudadano impone el artículo 95 de la

actividades peligrosas a los casos en que se causa daño por el uso de *DeepFakes*, su aplicación también presenta algunos inconvenientes.

De acuerdo con Jiménez (2025), uno de los principales desafíos del régimen actual es que los sistemas IA no son controlados ni supervisados por humanos, por lo que es difícil determinar quién tiene la guarda de la cosa causante del daño. "En efecto, la falta de control en los sistemas de IA se refiere a la dificultad o imposibilidad de influir en el comportamiento de un sistema o modelo, especialmente cuando este opera como una caja negra" (p. 204). En este sentido, la autora señala que se vuelve complejo probar la causalidad, la culpa y el nexo causal, lo que obstaculiza la imputación de responsabilidad[33].

Al respecto, autores como Rodrigo López (2022) han señalado que una de las alternativas para tratar los *DeepFakes* es estableciendo responsabilidad a las plataformas a través de las cuales estos se divulgan (p. 140). Lo anterior con base en la idea de que quienes ostentan los derechos de propiedad sobre las plataformas, tienen un deber de vigilancia sobre las mismas. No obstante, esta propuesta presenta dos inconvenientes: en primer lugar, esta alternativa no brindaría una solución real a los casos en los que se comparten *DeepFakes* sin acudir a plataformas digitales. En segundo lugar, la jurisprudencia constitucional ha proscrito la censura previa por considerar que vulnera el derecho a la libertad de expresión[34]. En esta misma línea, la

Constitución, sino particularmente, por las "implicaciones humanísticas que le son inherentes", al ejercicio de la medicina".

[33] Así mismo, Jimenez (2025) señala que "atribuir responsabilidad solidaria en todos los casos en los que esté involucrado un sistema de IA, por aplicación del criterio de la guarda de la cosa, no parece razonable […] en la medida en que, aun aplicándose la presunción de culpa por considerarse como una actividad peligrosa, el nexo causal tiene que ser probado por el accionante, como lo ha reconocido la jurisprudencia" (p. 205).

[34] En este sentido se pronunció la Corte Constitucional en la Sentencia T-243/18, con M.P. Diana Fajardo RIvera al señalar que "[...] en lo que tiene que ver con el contenido de lo que se da a conocer, esta libertad comprende toda comunicación de ideas, informaciones y opiniones, incluso si no resultan socialmente aceptables, incómodas ofensivas o contrarias al sentimiento mayoritario. En consecuencia, la libertad de expresión está sujeta únicamente a responsabilidades posteriores que responderán, exclusivamente, a la afectación de derechos fundamentales de terceras personas, es decir que está prohibida la censura previa".

Corte Suprema de Justicia ha dado aplicación al régimen subjetivo cuando se trata de daños causados por publicaciones en plataformas digitales[35].

En conclusión, si bien eventualmente podría considerarse la generación de *DeepFakes* como actividad peligrosa, para ello sería necesario apartarse de la interpretación la jurisprudencia ha dado tradicionalmente a dicho término. Adicionalmente, aun cuando se lograra catalogar esta actividad como peligrosa, se presentaría otro inconveniente: dada la complejidad de los sistemas de IA, resultaría difícil establecer a quién atribuir la responsabilidad; esto es, quien ostenta la calidad de actividad peligrosa. Por último, no debe perderse de vista que la jurisprudencia ha prohibido expresamente la censura previa con el fin proteger el derecho a la libertad de expresión, de modo que no podría acogerse un régimen que limitara de manera anticipada dicho derecho fundamental[36].

3.2.2.2 Responsabilidad por el hecho ajeno

Este régimen se encuentra previsto en el artículo 2347 del Código Civil. A través de esta figura es posible imputar el daño causado por un tercero a quien ejerce sobre él una relación de custodia, dirección o dependencia, como en el caso de los padres frente a los hijos menores. En este tipo de imputación, el tercero a quien es atribuible el daño puede librarse de responsabilidad si prueba que, aun con su autoridad, no habría podido impedir el hecho.

La doctrina y la jurisprudencia no han sido unánimes al establecer si este tipo de responsabilidad se enmarca en un régimen subjetivo u objetivo. De un lado, autores como

---

[35] Es el caso de la Sentencia SC5238-2019, en la cual se analizó la responsabilidad derivada de una publicación en un blog desde la óptica de la responsabilidad subjetiva.

[36] " [...] la discusión sobre limitar o no la garantía de la libertad de expresión en las plataformas digitales, se ha originado en situaciones donde la publicación de ciertos contenidos causan daños o agravios a terceros; sin embargo, por tratarse de una prerrogativa constitucional y cimiento de la democracia misma, cualquier reglamentación o fijación de subreglas jurisprudenciales debe ser cuidadosa de no afectarla, sobre todo en temas de interés público" (Corte Suprema de Justicia, Sentencia SC5238-2019)

Tamayo (2007) han establecido que se trata de un régimen objetivo, en tanto, si bien puede ser necesaria la culpa del directamente responsable, una vez probada se genera la responsabilidad del civilmente responsable, quien no puede exonerarse probando diligencia y cuidado (p. 237). De otro lado, la jurisprudencia ha dado a entender también que en estos casos el que se presume civilmente responsable puede exonerarse probando diligencia y cuidado:

> En estos eventos, la ley establece que los primeros, debido a la posición dominante que les otorga su autoridad, tienen el deber de impedir que los segundos actúen de forma imprudente, de suerte que si la conducta de éstos genera algún tipo de daño, la ley presume que ello ocurre por desatender u omitir su función de buenos vigilantes. El reproche de culpabilidad no se circunscribe en estos casos a analizar si hubo o no culpa en la producción del daño, sino a valorar la vigilancia que el superior ejerce sobre quien está bajo su cuidado. (Corte Suprema de Justicia, Sala de Casación Civil, *Sentencia SC13925-2016*, 24 de agosto de 2016, M. P. Ariel Salazar Ramírez)

Puesto que el presente trabajo se centra en la normatividad colombiana, asumimos la postura de que se trata de un caso de imputación subjetiva con presunción de culpa. Lo anterior, en tanto que la jurisprudencia indica que el civilmente responsable puede exonerarse de dicha responsabilidad si prueba diligencia; esto es, que cumplió cuidadosamente su deber de vigilancia.

La Responsabilidad por el Hecho Ajeno Aplicada a Casos de Daños Causados por Deepfakes.

La doctrina se ha planteado imputar responsabilidad bajo la figura de responsabilidad por el hecho ajeno en los casos de daños causados por robots. De acuerdo con Wigg (2024):

> La aplicación analógica de las normas de responsabilidad civil, por hecho ajeno a los daños causados por sistemas inteligentes, se apoya en el principio de equivalencia funcional. Este principio dicta que las víctimas deben ser tratadas como si la actividad dañosa hubiera sido realizada por un humano, argumentando que existen fundamentos similares para responsabilizar a

> una persona por daños causados tanto por sus dependientes humanos como por automatización avanzada (p. 256).

Sin embargo, cabe recalcar que robot e inteligencia artificial no son sinónimos. Según Porcelli (2020), la inteligencia artificial busca construir algoritmos capaces de resolver problemas que las personas solucionan a diario. En este sentido, pueden realizar funciones como lectura y procesamiento de datos, aprendizaje automático, entre otros. Si bien la inteligencia artificial puede aplicarse a los robots, estos dos conceptos no son sinónimos (pp. 57 - 70).

Dicho lo anterior se tiene que la posibilidad de aplicar "equivalencia funcional" tiene sentido si se habla de un robot con un grado importante de autonomía, que pueda determinarse no solo según el algoritmo, sino también según el entorno[37]. En contraste, el *DeepFake* es un tipo de inteligencia artificial que permite crear montajes hiperrealistas, pero lo hace según lo solicitado por el usuario. No posee una autonomía comparable a la humana[38].

Adicionalmente, Wigg (2024) también critica la idea de que los robots puedan actuar con culpa (p. 256). Sin embargo, la Corte Suprema de Justicia colombiana ha indicado que no debe ligarse el concepto de culpa con la idea de libre albedrío (Sentencia del 30 de septiembre de 2016). Dado lo anterior, toda vez que los sistemas de *DeepFake* no tienen un grado de autonomía tal que sea comparable con el de los humanos, difícilmente podría hablarse de responsabilidad por el hecho ajeno.

---

[37] Porcelli (2020) señala, se puede diferenciar entre los robots no autónomos que realizan tareas automatizadas; los autónomos y la inteligencia artificial aplicada a los robots que perciben el ambiente externo por sí mismos, sin necesidad de órdenes preprogramadas externas y con capacidad de discernir entre diferentes circunstancias que pueden acontecer a su alrededor. Estos sistemas deben obedecer tanto las órdenes de otros sistemas de inteligencia artificial como las humanas que interaccionan con él (p. 70).

[38] De acuerdo con Aguirre (2024) "Es el grado de autonomía que posee el robot, el que permite, la posible responsabilidad de los robots".

3.2.2.3 Responsabilidad por el Hecho de los Animales y las Cosas.

Los artículos 2350, 2353, 2354 y 2355 del Código Civil prevén supuestos de responsabilidad por el uso o tenencia de algunas cosas. Mientras que los artículos 2353 y 2354 tratan supuestos en los que los animales ya sean fieros o domésticos causan daños, los artículos 2350 y 2355 establecen el régimen de responsabilidad aplicable a las cosas que caen de los edificios o a la ruina misma de éstos. Ahora bien, en Colombia no existe, en sentido estricto, un régimen de responsabilidad por el hecho de las cosas, sino únicamente un par de hipótesis taxativas previstas en el Código Civil. No obstante, analizaremos la aplicabilidad de este tipo de régimen debido a que una parte de la doctrina ha considerado viable esta alternativa en materia de daños causados por la inteligencia artificial.

Respecto de la responsabilidad por animales fieros, la jurisprudencia ha establecido que para que haya responsabilidad en estos casos deben concurrir dos supuestos: "(i) La producción de un daño por un animal fiero y, a su vez, (ii) que el animal no reporte "utilidad para la guarda o servicio de un predio" (Corte Constitucional, *Sentencia C-111 de 2018*). Así mismo, ha señalado que en estos casos no es posible exonerarse de responsabilidad probando ausencia de culpa, sino sólo al demostrar la ausencia del nexo causal. En este sentido, se trata de una responsabilidad objetiva que se fundamenta en el riesgo creado por el dueño o guardián al tener un animal fiero que no reporta utilidad y es potencialmente peligroso (Sarmiento, 2024, p. 216).

En contraste, en el caso de los animales domésticos[39], el Código Civil prevé una presunción de culpa desvirtuable que recae sobre el propietario del animal o sobre quien tiene su custodia (Sarmiento, 2024, p. 216). Según Velásquez (2009) esta responsabilidad se fundamenta en la culpa *in vigilando* (p. 547). Sin embargo, este autor advierte que, tanto para algunos

[39] Artículo 2353 del Código Civil colombiano

doctrinantes como para la jurisprudencia, los daños causados por un animal extraviado pueden configurar supuestos de responsabilidad objetiva. En este sentido, señala que tanto la Corte Suprema de Justicia[40] como Martinez Rave[41] coinciden en que, cuando el daño ocurre mientras el animal está extraviado y dicho extravío no es atribuible al propietario ni al custodio se configura un régimen objetivo de responsabilidad en el cual solo es posible exonerarse acreditando una causa extraña. No obstante, Velásquez (2009) discrepa de esta idea, al considerar que el 2353 exige la existencia de culpa, ya sea en el extravío o el daño. De lo que se infiere que si no hay culpa en el extravío entonces no es posible imputar culpa en el daño, lo que excluye la responsabilidad (p. 549).

Por último, en cuanto a la responsabilidad por las cosas inanimadas, en primer lugar, el artículo 2350[42] prevé que el dueño de un edificio en ruinas es responsable por los daños que este cause, ya sea porque se omitieron reparaciones necesarias o porque fue negligente de alguna forma. Al respecto, Velasquez (2009) señala que se trata de un supuesto de responsabilidad subjetiva; no obstante, indica que esto no es aceptado por todos en la doctrina, y que, para Valencia Zea, por ejemplo, solo es posible exonerarse de responsabilidad probando caso fortuito, se trataría entonces de un supuesto de responsabilidad objetiva (p. 553).

En segundo lugar, el artículo 2355[43] prevé la responsabilidad por objetos que caen de edificios. En este sentido tampoco hay una posición unánime en la doctrina respecto de la naturaleza de dicho régimen en cuanto a una responsabilidad objetiva o subjetiva. Al respecto, Velásquez (2009), cita a Martinez Rave, quien argumenta que se trata de un supuesto de

[40] Corte Suprema de Justicia, Sala de Casación Civil. (1976)
[41] Velasquez(2009) cita a Martinez Rave
[42] Artículo 2350 del Código Civil colombiano
[43] Artículo 2355 del Código Civil colombiano

responsabilidad objetiva en tanto la víctima no tiene que probar la culpa de los habitantes del edificio y, al contrario, el mismo Velásquez sostiene que se trata más bien de una responsabilidad por culpa presunta, desvirtuable si se prueba que el daño se debió a la culpa o dolo de una persona específica (Rave, 1998, como se citó en Velásquez, p. 560).

Responsabilidad por el hecho de las cosas y los animales aplicada a los casos en que se causan daños por el uso de DeepFakes.

De acuerdo con Wigg (2024) hay quienes proponen que los robots sean considerados como análogos a los animales o las cosas. Al respecto, la autora expone que, así como el dueño de animales carga con el riesgo inherente a su tenencia, hay quienes consideran que los dueños de robots inteligentes deberían correr con la misma suerte. No obstante, en este punto la autora señala que difícilmente pueden compararse:

> Aun cuando ambos entrañan un peligro incontrolable por su dueño o poseedor, los robots operan bajo parámetros de programación y algoritmos definidos por humanos, incluyendo los modelos avanzados de autoaprendizaje. Sus "acciones" derivan de códigos y datos, no de un instinto o voluntad propia como en los animales. Los animales actúan con base en instintos, necesidades y respuestas a su entorno, que pueden ser predecibles hasta cierto punto, pero no están preprogramadas. En resumen, aunque máquinas y animales pueden comportarse de maneras imprevisibles, no es por la misma causa. En animales, la imprevisibilidad puede estar relacionada con su naturaleza y es influenciada por su biología y entorno. En robots, la imprevisibilidad puede surgir de errores de programación, fallos en el hardware, o comportamientos emergentes no anticipados por los diseñadores. (p. 257)

Al respecto, resulta útil indicar que, si se presentan estas discusiones en materia de robots autónomos, difícilmente podría hacerse una analogía entre la IA (*DeepFake* específicamente) y los animales. Como se indicó anteriormente, el aprendizaje automático de los *DeepFakes* no

implica que estos sistemas actúen con autonomía, sino que una tecnología generativa perfecciona sus habilidades para lograr un propósito específico; esto es, crear material audiovisual que sea indistinguible y pueda confundirse con la realidad. Si bien es posible que estos sistemas cometan errores y por tanto el resultado no sea tal cual lo esperaba el usuario, está claro que en este tipo de IA no se puede hablar de un agente autónomo que, por ejemplo, por iniciativa produzca *DeepFakes* que causen daños a terceros.

No obstante, resulta relevante destacar lo señalado por Kelley et al. (2010). Estos autores proponen que, en el caso de los robots, si estos no tienen problemas de fábrica, entonces el responsable por los daños que los mismos causen será el dueño (si se prueba su culpa). Esta explicación la plantean a partir de una analogía con la responsabilidad por animales domésticos (p. 4). Respecto a este punto, Cárdenas y Gómez (2020) señalan que la idea parece más aplicable a la responsabilidad por el hecho de las cosas inanimadas que por el hecho de los animales[44](p. 78). No obstante, al analizar los elementos de la responsabilidad por los animales o las cosas en el contexto colombiano, la posición propuesta no parece encajar en ninguno de los regímenes señalados[45].

Por un lado, respecto a la responsabilidad por animales domésticos, se tiene que, como se indicó, tecnologías como el *DeepFake* no son comparables con un animal. No gozan de un grado siquiera similar de autonomía y, por tanto, no sería posible aplicar una analogía entre categorías. Por otro lado, respecto a la responsabilidad por el hecho de las cosas tampoco parece aplicable la

[44] Al respecto, cabe resaltar que los autores que propusieron la interpretación planteada lo hicieron en el contexto estadounidense.

[45] Con la salvedad previamente expuesta de que no existe como tal un régimen de responsabilidad por el hecho de las cosas en Colombia.

teoría planteada pues, como se explicó previamente, en Colombia solo se ha previsto esta figura para situaciones específicas[46].

3.2.2.4 Responsabilidad por productos defectuosos

La Ley 1480 de 2011; esto es, el actual estatuto del consumidor prevé un régimen especial de responsabilidad que protege a los consumidores y presume la responsabilidad del productor o proveedor ante los daños causados por un producto defectuoso. De acuerdo con Espinosa (2015) el régimen de responsabilidad por productos defectuosos[47] se fundamenta en una obligación legal y constitucional[48] de seguridad y de resultado, que se impone a productores y proveedores sin necesidad de un vínculo contractual (p. 378).

De acuerdo con el artículo 6 del Estatuto del consumidor, todo productor debe garantizar la calidad, seguridad e idoneidad de los bienes y servicios que ofrezca. Así mismo, esta misma disposición prevé que el incumplimiento de esta obligación da lugar, entre otras, a la responsabilidad por productos defectuosos. Este tipo de responsabilidad es explicada por Espinosa (2015) como:

> Responsabilidad solidaria frente al consumidor, a cargo del productor y el proveedor, en razón de la ausencia de seguridad en los productos que ponen en circulación. Para el consumidor, se traduce en una pretensión indemnizatoria de los perjuicios ocasionados por productos defectuosos en su persona y sus bienes, que se hace valer a través de una acción jurisdiccional únicamente ante la jurisdicción ordinaria, sea individualmente, sea a través de una acción de grupo. (p. 382)

---

[46] De acuerdo con Wigg (2024) “las reglas de responsabilidad por hechos de las cosas son específicas y no se adecúan fácilmente a los robots”. (p. 257)

[47] El artículo 5 de la Ley 1480 de 2011 define los productos defectuosos en el numeral 17 como: “aquel bien mueble o inmueble que en razón de un error el diseño, fabricación, construcción, embalaje o información, no ofrezca la razonable seguridad a la que toda persona tiene derecho”

[48] Constitución política de Colombia, artículo 78, inciso 2.: Serán responsables, de acuerdo con la ley, quienes en la producción y en la comercialización de bienes y servicios, atenten contra la salud, la seguridad y el adecuado aprovisionamiento a consumidores y usuarios.

La jurisprudencia de la Corte Suprema de Justicia ha establecido que para que se configure responsabilidad por productos defectuosos deben cumplirse 3 elementos: el daño, el defecto del producto, y la relación de causalidad entre ambos[49]. De lo anterior, se desprende que la jurisprudencia[50] y una parte de la doctrina, en cuanto a la naturaleza de este régimen, han opinado que se trata de una responsabilidad objetiva[51]. Sin embargo, de acuerdo con Ortega et al. (2024) se han planteado dos posibles contraargumentos frente a la naturaleza objetiva de este régimen de responsabilidad. El primero se apoya en la definición de producto defectuoso establecida en la Ley 1480 de 2011, que emplea el término "error" para referirse a las razones por las cuales los bienes muebles o inmuebles no garantizan el nivel de seguridad razonable que toda persona tiene derecho a esperar (artículo 5.17). El segundo refiere que el empresario puede exonerarse si demuestra que, al momento de poner el producto en circulación, el estado del arte no permitía conocer el defecto, por lo que no se trataría de un régimen objetivo (pp. 392 - 393).

Régimen de responsabilidad por productos defectuosos en los casos de daños causados por DeepFakes.

[49] Así lo prevé, entre otras, la sentencia de la Corte Suprema de Justicia, Sala de Casación Civil. (2009, 24 de septiembre). *Sentencia Exp. 05360-31-03-001-2005-00060-01*. Magistrado ponente: César Julio Valencia Copete. Bogotá, Colombia, que reitera la sentencia de la Corte Suprema de Justicia, Sala de Casación Civil. (2009, 30 de abril). *Sentencia Exp. 25899 3193 992 1999 00629 01*. Magistrado ponente: Pedro Octavio Munar Cadena. Bogotá, Colombia. Estas sentencias si bien fueron expedidas antes de la promulgación de la ley 1480 de 2011, tienen sus bases en el mandato constitucional del artículo 78 de la Constitución política.

[50] La jurisprudencia ha reconocido que se trata de un régimen objetivo en sentencias como la Corte Constitucional, Sala Plena. Sentencia C-1141 de 2000. M.P: Eduardo Cifuentes Muñoz (30 de agosto de 2000), Corte Suprema de Justicia, Sala de Casación Civil. (2009, 30 de abril). *Sentencia Exp. 25899 3193 992 1999 00629 01*. Magistrado ponente: Pedro Octavio Munar Cadena. Bogotá, Colombia, Corte Suprema de Justicia, Sala de Casación Civil. (2009, 24 de septiembre). *Sentencia Exp. 05360-31-03-001-2005-00060-01*. Magistrado ponente: César Julio Valencia Copete. Bogotá, Colombia.

[51] Es el caso de Brenda Espinosa Apráez (2015) que platea que "se desprende que en el ámbito de la responsabilidad por producto defectuoso es indiferente si el productor o el proveedor obraron con culpa, lo cual puede corroborarse además con el hecho de que el estatuto no requiere que el afectado pruebe tal circunstancia para estructurar esta responsabilidad, pues de conformidad con el artículo 21 de la Ley 1480 de 2011, para que esta pueda establecerse, el afectado deberá demostrar el defecto del bien, la existencia del daño y el nexo causal entre este y aquel, omitiendo toda referencia a la culpa del empresario" (pp. 391-392).

Autores como Kelley, et al. (2010) han propuesto tratar a los robots como productos y acudir al régimen de responsabilidad por productos defectuosos en los casos en que la causación de daños sea atribuible a un defecto del producto (p. 3). Sin embargo, esta propuesta ha sido planteada para el ámbito de la robótica.

Al respecto, Wigg (2024) advierte que uno de los principales retos de aplicar la responsabilidad por productos defectuosos a los casos en que se causan daños por el uso de IA radica en la definición de "producto defectuoso". Lo anterior, en tanto la norma define el producto defectuoso como "bien mueble o inmueble", y no es claro que la IA se pueda clasificar como tal[52]. No obstante, Wigg señala que para la mayoría de los autores europeos la IA sí constituye un producto. En el presente trabajo se asumirá dicha posición[53] (pp. 251 - 252).

Para analizar la aplicabilidad del régimen de productos defectuosos en los casos de daños causados por *DeepFakes* es importante empezar por establecer en qué eventos podría considerarse que la IA constituye un producto defectuoso. Wigg (2024) señala que los productos se consideran defectuosos cuando no ofrecen la seguridad razonable que se podría esperar de ellos, sin embargo, este aspecto es complicado de determinar en tecnologías complejas. Al respecto, la autora señala que, para afrontar dichas dificultades, Estados Unidos adoptó el *Risk-Utility test*, que limita los riesgos del fabricante a los defectos que ocasionen daños que podrían haberse evitado o reducido mediante un diseño alternativo (pp. 252 - 253).

En el caso colombiano, la jurisprudencia ha indicado que un producto es defectuoso:

> […] cuando **no ofrece la seguridad que legítimamente se espera de él**, condición que… se predica no por su falta de aptitud para el uso para el que fue adquirido, sino por no cumplir las

[52] Cabe aclarar que la autora es Chilena, sin embargo,Colombia y Chile comparte la definición de producto defectuoso en ese aspecto.

[53] No se entrará en detalles respecto a esta discusión, pues esto excedería los objetivos del presente trabajo.

> condiciones de seguridad a que tiene derecho el público", **ámbito del cual escapa, desde luego, la utilización abusiva (**...) puede ocurrir, igualmente, que a pesar de ser idóneo el producto sea defectuoso", como "**cuando carece de las instrucciones necesarias para su adecuada y confiable utilización**" o "por deficiencias del embalaje pone en riesgo al consumidor"; y es claro, por supuesto, que "la obligación de seguridad cuyo incumplimiento genera el deber indemnizatorio de que aquí se trata es aquella a la que razonablemente se puede aspirar", de donde quedan "**excluidas las situaciones en las que el carácter riesgoso del producto es aceptado o conocido por el público**"(Corte Suprema de Justicia, Sala de Casación Civil, *Sentencia del 30 de abril de 2009, Exp. 1999-00629-01*, citada en la *Sentencia del 24 de septiembre de 2009, Rad. 2005-00060*)

Se observa, por tanto, que un producto, a pesar de ser "idóneo" puede ser defectuoso si carece de las instrucciones necesarias. Al respecto, el artículo 23 del Estatuto del Consumidor establece que:

> Los proveedores y productores deberán suministrar a los consumidores información, clara, veraz, suficiente, oportuna, verificable, comprensible, precisa e idónea sobre los productos que ofrezcan y, sin perjuicio de lo señalado para los productos defectuosos, serán responsables de todo daño que sea consecuencia de la inadecuada o insuficiente información

En este mismo sentido se pronuncia la sentencia del 24 de septiembre de 2009, *Rad. 2005-00060*, en la cual la Corte Suprema de Justicia señaló que:

> En este sentido, podrá ser defectuoso el producto frente al cual no se ofrece al consumidor la información que a su cargo tiene el fabricante, ya se trate de aquella que debe suministrar con el envase, envoltura o presentación respectiva ora de la complementaria que deba canalizar a través de los diversos medios de publicidad, referida a aspectos como el modo en que ha de ser empleada, a las precauciones o advertencias relativas a su uso razonable; en fin, toda la

información que sea necesaria de tal manera que no resulte lesionada la seguridad que todo consumidor legítimamente ha de esperar del producto.

Bajo este entendido, el régimen de responsabilidad por productos defectuosos podría tener aplicación en los casos en que se omita dar instrucciones respecto a cómo debe usarse la tecnología de *DeepFakes* y las posibles consecuencias de su mal uso. No obstante, es necesario analizar también los otros supuestos señalados por la Corte; esto es, los casos de utilización abusiva y si el carácter riesgoso del producto es conocido y aceptado.

En relación con el primer punto, si bien la Corte no definió a qué se refería con uso abusivo, esta puede vincularse con la noción de abuso del derecho. De acuerdo con la Corte Constitucional en la sentencia SU631-17 del 12 de octubre de 2017, el abuso del derecho se configura cuando su titular ejerce una facultad o garantía subjetiva contradiciendo los fines de esta, o cuando en el ejercicio de un derecho se desbordan los límites que el ordenamiento jurídico impone. Bajo esta perspectiva, no habría responsabilidad a cargo del productor o proveedor si, por ejemplo, los daños se causaron por que el usuario, pese a las instrucciones brindadas, decidió contravenirlas y causó un daño.

En cuanto al segundo punto, es necesario analizar si se puede afirmar que el carácter riesgoso de los *DeepFakes* es conocido y aceptado por el público. Al respecto, si bien hay literatura y doctrina sobre *DeepFakes*, consideramos que difícilmente se puede afirmar que sus riesgos son conocidos y aceptados por la generalidad de las personas. Hay que tener en cuenta, que la generalidad de las personas no conoce siquiera el funcionamiento de estos sistemas y que el consumidor se encuentra en condiciones de inferioridad en relación con el productor o prestador, en especial en materia de tecnologías tan complejas como esta[54].

[54] De acuerdo con la Corte Constitucional "[…] la razón de ser de este régimen estriba en la necesidad de compensar con medidas de distinto orden la posición de inferioridad con que consumidores y usuarios, por lo general dispersos

En conclusión, consideramos que este régimen es una alternativa viable para imputar responsabilidad, no obstante, es necesario establecer ciertas claridades: en primer lugar, esto solo podría brindar una solución en los casos en que se incumplió con el deber de información. En segundo lugar, si bien este régimen facilita la tarea a la víctima en tanto productor y proveedor responden solidariamente, no soluciona lo relativo a la relación entre productores y proveedores.

4. Conclusiones

A partir de lo expuesto a lo largo del presente trabajo, puede afirmarse que los *DeepFakes* son una de las representaciones más avanzadas de la inteligencia artificial en la manipulación audiovisual. Así mismo, se señaló que, aunque esta tecnología tiene su uso legítimo en campos como la educación, el arte o la salud, su uso indebido plantea riesgos jurídicos graves que pueden vulnerar derechos personalísimos y producir daños morales y/o patrimoniales profundos. Adicionalmente se aclaró que, en los casos de *DeepFake*, la gravedad del daño no depende de la veracidad del contenido sino su impacto social y subjetivo. Dado esto, se ha establecido que es necesario que el ordenamiento jurídico reconozca tanto el potencial creativo de dicha tecnología como sus peligros y, por lo tanto, se utilice para proporcionar mecanismos efectivos de prevención, protección y reparación.

Con el propósito de tener referencias internacionales respecto al trato que se ha dado a la problemática de los *DeepFakes*, se analizaron los métodos utilizados por Corea del Sur, Estados Unidos y la Unión Europea. A partir del análisis comparativo realizado, se puede concluir que las respuestas legales se muestran disímiles, aunque la mayoría de los países han recurrido a reformas legislativas para abordar el problema de los *DeepFakes*.

---

y dotados de escasos conocimientos y potencialidades, enfrentan a las fuerzas de la producción y comercialización de bienes y servicios, necesarios en orden a la satisfacción de sus necesidades materiales". (Sentencia 1141 del 2000)

En el caso de Corea del Sur se actualizó la Ley de Delitos Sexuales para incluir como delito la fabricación de *DeepFakes* con contenido sexual no consensuado. Sin embargo, en materia civil no se ha creado una regulación específica, sino que se ha dado aplicación al régimen de responsabilidad con el que ya se contaba; es decir, las víctimas pueden acudir a la cláusula general de responsabilidad extracontractual, así como a la jurisprudencia sobre derechos de imagen e intimidad, combinando estas acciones con los procesos penales para reforzar la reparación.

Situación similar se observa en Estados Unidos, donde California y Texas han reiniciado recientemente sus códigos electorales y se han venido presentando proyectos de ley relativos a la regulación de estas tecnologías. Estos métodos van acordes con lo que la jurisprudencia estadounidense ha referenciado. De acuerdo con esta, debido a las protecciones previstas en la primera enmienda, no es posible prohibir los *DeepFakes* falsos en general, sino solo para situaciones específicas en que se presenten daños jurídicamente reconocibles que encajen en figuras no protegidas por la primera enmienda como lo son la difamación, el fraude, las amenazas verdaderas o la incitación inminente a la violencia.

Por el contrario, la Unión Europea prevé marcos regulatorios generales acompañados de directivas específicas que los estados miembros deben implementar en la legislación nacional (por ejemplo, la Regulación de IA y la DSA). En este sentido, Europa, con el fin de tener una regulación específica en materia de inteligencia artificial, ha hecho lo opuesto a reformular las normas actuales. En este contexto, dispuso una norma marco para dar tratamiento jurídico a estas nuevas tecnologías, y ha previsto que los *DeepFakes* son IA con riesgos de manipulación, por lo que quien haga uso de ellos debe aclarar que se trata de producciones manipuladas o creadas con IA.

Una vez revisadas estas alternativas internacionales, se estudiaron algunos conceptos clave para entender someramente el régimen de responsabilidad civil extracontractual en Colombia y, posteriormente, se expusieron las generalidades de ciertos regímenes de responsabilidad. De dicho análisis se concluyó que sería viable atribuir responsabilidad a través de un régimen subjetivo, del régimen de responsabilidad por actividades peligrosas y del régimen de responsabilidad por productos defectuosos.

Respecto del régimen subjetivo, se estableció que este sería viable en el entendido de que en Colombia está prohibido, por regla general, el tratamiento de datos sin autorización de su titular y, adicionalmente, los principios en materia de tratamiento de datos exigen la veracidad y calidad de los mismos. Sin embargo, se señaló que este régimen presenta un problema en tanto no es claro a quien se le atribuye el actuar culposo, asunto que es fundamental para atribuir responsabilidad. No obstante, también se indicó que esta problemática podría resolverse acudiendo a un análisis de la causalidad o una analogía con lo previsto en la Ley Penal, según la cual la responsabilidad se atribuye a quién saque provecho de la suplantación de identidad.

En cuanto al régimen de responsabilidad por actividades peligrosas, señalamos que este también podría ser útil en cuanto la creación de *DeepFakes* podría considerarse como tal. No obstante, se precisó que, en este ámbito, se produciría un problema para establecer quién es el guardián de la actividad peligrosa. Así mismo, la jurisprudencia no podría aplicar interpretaciones que limitaran el derecho a la libertad de expresión.

Por último, en lo relativo al régimen de responsabilidad por productos defectuosos, consideramos que este también podría brindar una solución en los casos en que la IA pueda considerarse como tal. En este aspecto, señalamos que, si consideramos los proveedores del servicio (entiéndase desarrolladores o quienes ostentan el derecho sobre el software) tienen un

deber de información respecto al riesgo representado por los *DeepFakes* y este se incumple, sería viable aplicar responsabilidad por daños causados por productos defectuosos.

5. Bibliografía

Aguilar-Castañeda, M. (2018). *La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados*.https://hdl.handle.net/10983/23060

Anuario de la Facultad de Derecho(2024). Dykinson. https://www-digitaliapublishing-com.ezproxy.eafit.edu.co/a/172592

Ariza Fortich, A. (2013). La responsabilidad médica como actividad peligrosa: Análisis de caso en la jurisprudencia de la Corte Suprema de Justicia de Colombia. *Vniversitas, 126,* 15–37.

Baena Aramburo, F. (2021). *La causalidad en la responsabilidad civil.* Tirant lo Blanch.

Briones, H. P. J., Zevallos Loyaga, M. E., Segura Grados, A. Y., & Castrejon Vilchez, E. M. (2024). El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el DeepFake. *Vniversitas, 73*, 1-28. https://doi.org/10.11144/Javeriana.vj73.uiti

Cambridge Dictionary. (s. f.). En *Cambridge Dictionary*. Recuperado el 20 de septiembre de 2025, https://dictionary.cambridge.org/dictionary/english/DeepFake

Cárdenas Gallagher, D. A., & Gómez Gutiérrez, V. (2020, septiembre). *Responsabilidad civil extracontractual de la inteligencia artificial en el régimen jurídico colombiano: ¿Necesidad de un cambio normativo?* [Tesis de pregrado, Pontificia Universidad Javeriana]. Repositorio Institucional, Pontificia Universidad Javeriana. http://hdl.handle.net/10554/51579

Citron, D. K. (2019). Sexual Privacy. *Yale Law Journal, 128*, 1870–1917. https://scholarship.law.bu.edu/faculty_scholarship/620

Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*, 1753-1819. https://scholarship.law.bu.edu/faculty_scholarship/640

Colombia, Congreso de la República. (1982, enero 28). *Ley 23 de 1982: Sobre derechos de autor*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3431

Colombia, Congreso de la República. (2012, octubre 17). *Ley Estatutaria 1581 de 2012:* Por la cual se dictan disposiciones generales para la protección de datos personales.

Constitución Política de Colombia. Art. 1 y 5 .Julio 7 de 1991 (Colombia).

Corte Constitucional de Colombia. (2007, mayo 24). *Sentencia T-405/07* (M.P. Jaime Córdoba Triviño).

Corte Constitucional de Colombia. (2017, octubre 12). *Sentencia SU631-17* (M. P. Gloria Stella Ortiz Delgado).

Corte Constitucional de Colombia. (2018, octubre 17). *Sentencia C-111 de 2018* (M. P. Alejandro Linares Cantillo)

Corte Suprema de Justicia, Sala de Casación Civil. (2001, enero 30). *Sentencia Exp. 5507* (M. P. José Fernando Ramírez Gómez).

Corte Suprema de Justicia, Sala de Casación Civil. (2004, marzo 3). *Sentencia Exp. C-7623* (M. P. José Fernando Ramírez Gómez).

Corte Suprema de Justicia, Sala de Casación Civil. (2009, abril 30). *Sentencia Exp. 25899-3193-992-1999-00629-01* (M. P. Pedro Octavio Munar Cadena).

Corte Suprema de Justicia, Sala de Casación Civil. (2009, septiembre 18). *Sentencia 20001-3103-005-2005-00406-01* (M. P. William Namén Vargas).

Corte Suprema de Justicia, Sala de Casación Civil. (2009, septiembre 24). *Sentencia Exp. 05360-31-03-001-2005-00060-01* (M. P. César Julio Valencia Copete).

Corte Suprema de Justicia, Sala de Casación Civil. (2019, diciembre 10). *Sentencia SC5238-2019* (Rad. 76001-31-03-015-2011-00088-02) (M. P. Luis Armando Tolosa Villabona).

Corte Suprema de Justicia, Sala de Casación Civil. (2016, septiembre 30). *Sentencia SC13925-2026* (Rad. 05001-31-03-003-2005-00174-01) (M.P. Ariel Salazar Ramirez).

Corte Suprema de Justicia, Sala de Casación Civil. (2020, noviembre 25). *Sentencia SC5176-2020* (Rad. 11001-31-03-028-2006-00466-01) (M. P. Luis Armando Rico Puerta).

Corte Suprema de Justicia, Sala de Casación Civil. (2021, septiembre 22). *Sentencia SC4204-2021* (Rad. 05001-31-03-003-2004-00273-02) (M. P. Álvaro Fernando García Restrepo).

Corte Suprema de Justicia, Sala de Casación Civil. (1976, marzo 11). *Sentencia del 11 de marzo de 1976* (M. P. José María Esguerra Samper).

Corte Suprema de Justicia, Sala de Casación Civil. (2023, marzo 27). *Sentencia SC065-2023* (Rad. 05001-31-03-005-2010-00259-01) (M. P. Hilda González Neira).

Courtis, C. (2019). *El juego de los juristas. Ensayo de caracterización de la investigación dogmática.* Universidad de Buenos Aires/ Instituto Tecnológico Autónomo de México.

Espinosa Apráez, B. (2015). La responsabilidad por producto defectuoso en la Ley 1480 de 2011: Explicación a partir de una obligación de seguridad de origen legal y constitucional. *Revista de Derecho Privado*, (28), 367–399. https://doi.org/10.18601/01234366.n28.11

Flórez Peláez, J., & Díaz Díez, C. A. (2022). *Imputación de daños causados por robots con inteligencia artificial: Conceptos aplicables de la responsabilidad civil y del Estado*. Centro de Estudios Regulatorios. https://www.cerlatam.com/publicaciones/imputacion-de-

danos-causados-por-robots-con-inteligencia-artificial-vigencia-de-los-presupuestos-tradicionales-de-la-responsabilidad-civil-y-del-estado/

Geng, Y. (2023). Comparing "*DeepFake*" regulatory regimes in the United States, the European Union, and China. *Georgetown Law Technology Review, 7*, 157-179

Gieseke, A. P. (2020). "The New Weapon of Choice": Law's Current Inability to Properly Address *DeepFake* Pornography. *Vanderbilt Law Review, 73*(5), 1479-1515. https://scholarship.law.vanderbilt.edu/vlr/vol73/iss5/4

Lee, C.-h., & Kim, D.-m. (Creadores). (2024). *A killer paradox* [Serie]. Netflix. https://www.netflix.com/co-en/title/81607354

Ley 2502 de 2025. Por medio de la cual se modifica y establece un agravante al artículo 296 de la Ley 599 de 2000, Código Penal Colombiano y se dictan otras disposiciones. Julio 28 de 2025. DO. N.° 53198.

Harris, D. (2019). *DeepFake*s: False pornography is here and the law cannot protect you. *Duke Law & Technology Review, 17*, 99–127.

Herrera de las Heras, R. (2022). *Aspectos legales de la inteligencia artificial: Personalidad jurídica de los robots, protección de datos y responsabilidad civil*. Dykinson. https://www-digitaliapublishing-com.ezproxy.eafit.edu.co/a/115845

Jiménez Mahecha, L. F. (2025). La responsabilidad contractual y extracontractual en el laberinto de la inteligencia artificial: Perspectiva colombiana. *Revista de Derecho Privado*, 24(2). https://doi.org/10.18601/16923960.v24n2.07

Kelley, R., Schaerer, E., Gomez, M., & Nicolescu, M. (2010). Liability in robotics: An international perspective on robots as animals. *Advanced Robotics, 24*(13), 1861–1871.

https://www.researchgate.net/publication/220671676_Liability_in_Robotics_An_International_Perspective_on_Robots_as_Animals

Kim, H. (Producer), & Kim, H., & Jeon, J. (Directors). (2020). *[I met you]* [TV documentary]. MBC.

Kosinski, J. (Director). (2020). *Top Gun: Maverick* [Película]. Paramount Pictures.

López, J. F. R. (2022). Tragic Realism: How to regulate *DeepFake*s in Colombia? *Latin American Law Review*, (8), 125–145. https://doi.org/10.29263/lar08.2022.08

Morales Neira, M. L. (2020). Uso y divulgación de la imagen personal: enfoques en el Derecho romano, en el Derecho colombiano y su actual interacción con la inteligencia artificial. *Revista de la propiedad inmaterial*, (30), 169–197. https://doi.org/10.18601/16571959.n30.07

Ortega, P., Vargas, J. C., Suaza, T., Nova, D., & Pérez, D. (2024). *Aplicación y límites del régimen de responsabilidad civil por producto defectuoso en el derecho colombiano*. Semillero de Investigación de Responsabilidad Civil y Seguros, Universidad de los Andes. https://derecho.uniandes.edu.co/wp-content/uploads/2024/05/producto-defectuoso.pdf

Ortiz Fernández, M. (2024). La adaptación del derecho de daños a la inteligencia artificial: La propuesta de Directiva sobre responsabilidad. *Revista de Derecho Privado, Universidad Miguel Hernández de Elche*.

Ortiz Figueroa, M. A., & Ortiz Flórez, J. S. (2024). Responsabilidad civil en la era digital: Daños causados por inteligencia artificial. *Genética y Derecho – Universidad Externado de Colombia.* https://geneticayderecho.uexternado.edu.co/responsabilidad-civil-en-la-era-digital-danos-causados-por-inteligencia-artificial/

Oxford English Dictionary. (s.f.). *Oxford English Dictionary*. https://www.oed.com/dictionary/deepfake_n?tab=meaning_and_use#1345352340

Pardo Rueda, R. (Creador), Samper Ospina, D, & Gutiérrez, J. A. (Productor). (2025). *La voz de Pardo* [Pódcast]. Escuela Digital. Disponible en plataformas digitales (Spotify; YouTube)

Porcelli, A. M. (2020). La inteligencia artificial y la robótica: Sus dilemas sociales, éticos y jurídicos. *Derecho Global. Estudios sobre Derecho y Justicia, 6*(16), 49–105. https://doi.org/10.32870/dgedj.v6i16.286

Roh, E. J. (2024). *[Análisis de la situación regulatoria de los DeepFakes a nivel nacional e internacional]* (KISDI Issue Report No. 4). Korea Information Society Development Institute.

Roh, E. J. (2025). *A Constitutional Study on DeepFake Expression*. [Tesis de doctorado, Sungkyunkwan University]

Rojas-Quiñones, S., & Mojica-Restrepo, J. D. (2014). De la causalidad adecuada a la imputación objetiva en la responsabilidad civil colombiana. *Vniversitas, 129*, 187–235. https://doi.org/10.11144/Javeriana.vj129.caio

Royer, S., Oerlemans, J.-J., & van Wegberg, R. (2024). An empirical and legal analysis of sexual DeepFakes in the EU, Belgium and the Netherlands. *Revue Internationale de Droit Penal, 95*(2), 459–482. https://scholarlypublications.universiteitleiden.nl/handle/1887/4198794

Sarmiento García, M. (2024). *Estudios de responsabilidad civil*. Universidad Externado de Colombia. https://www.digitaliapublishing.com/a/171485

Spivak, R. (2019). DeepFakes: The newest way to commit one of the oldest crimes. *Georgetown Law Technology Review, 3*, 339–390

Tamayo Jaramillo, J. (2007). *Tratado de responsabilidad civil* (Tomo I, 2.ª ed.). Legis.

Trigo Represas, F. A., & López Mesa, M. J. (2004). *Tratado de responsabilidad civil: El derecho de daños en la actualidad: teoría y práctica* (Tomo 1). La Ley.

United States of America. (1789). *Constitution of the United States: Amendment I*. National Archives. https://constitution.congress.gov/constitution/amendment-1/

Vallespín Pérez, D. (2025). Responsabilidad civil extracontractual en materia de IA: especial referencia a la carga de la prueba y la aplicación de presunciones. *IDP: Revista de Internet, Derecho y Política, (42).* Universitat de Barcelona. https://doi.org/10.7238/idp.v0i42.432054

Velásquez Posada, J. (2009). *Responsabilidad civil extracontractual*. Universidad de la Sabana. https://www.digitaliapublishing.com/a/18585

Wigg Sotomayor, I. (2024). Panorama del fenómeno de la inteligencia artificial en relación con la responsabilidad civil [Overview of the phenomenon of artificial intelligence in relation to civil liability]. *Actualidad Jurídica*, (50), 245–263. Universidad del Desarrollo. https://derecho.udd.cl/actualidad-juridica/files/2024/09/9-isabel-wigg-sotomayor.pdf