Universidad Andina Simón Bolívar

Sede Ecuador

Área de Derecho

Maestría en Derecho y Sociedad

Mención en Identidades y Acción Colectiva

IA en manos peligrosas

Impactos jurídicos de los *deepfakes* pornográficos

Daniela Carolina Cango Cango

Tutor: Juan Carlos Mejía Mediavilla

Quito, 2026

Trabajo almacenado en el Repositorio Institucional UASB-DIGITAL con licencia Creative Commons 4.0 Internacional

Reconocimiento de créditos de la obra

No comercial

Sin obras derivadas

creative commons

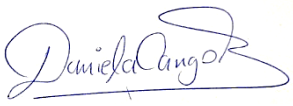
Para usar esta obra, deben respetarse los términos de esta licencia

Cláusula de cesión de derecho de publicación

Yo, Daniela Carolina Cango Cango, autora del trabajo intitulado “IA en manos peligrosas: Impactos jurídicos de los *deepfakes* pornográficos”, mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster en Derecho y Sociedad, Mención Identidades y Acción Colectiva en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en internet.
2. Declaro que, en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autora de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

23 de abril de 2026

Firma: 

Resumen

Los *deepfakes* representan una de las preocupaciones más urgentes en la sociedad contemporánea. Estas creaciones artificiales, generadas a través de la manipulación avanzada de imágenes y vídeos, han afectado gravemente tanto a figuras públicas como a personas particulares. Su origen se vincula al desarrollo de redes neuronales profundas propias de la inteligencia artificial generativa [en adelante IA generativa]. En particular, los *deepfakes* pornográficos han generado un grave impacto en los derechos de las personas, a través de técnicas de ingeniería social se ha vulnerado la dignidad en entornos digitales, cuyos contenidos falsos han sido divulgados en las diferentes plataformas de redes sociales.

El avance de las TIC y la IA han posibilitado la creación de *deepfakes*, pero su uso indebido ha generado riesgos significativos para la seguridad y privacidad *online*. Ante esta problemática, el *soft law*, mediante principios éticos y estrategias de educación digital, busca promover una conciencia crítica sobre el manejo responsable de la IA y el respeto a los derechos fundamentales en entornos virtuales. Sin embargo, cuando estas medidas no logran contener los abusos, el *hard law* cobra relevancia como un mecanismo de regulación vinculante, que busca garantizar una protección efectiva frente a las vulneraciones cometidas a través de la tecnología.

Desde una perspectiva jurídica, se ha visto que los *deepfakes* pornográficos vulneran derechos constitucionales, como la dignidad humana, privacidad y el honor de las personas afectadas. En el ámbito penal, esta tecnología compromete gravemente la intimidad, integridad e indemnidad sexual, lo que exige una respuesta firme y proporcional. Frente a estos desafíos, resulta urgente fortalecer los marcos regulatorios y fomentar una conciencia pública crítica sobre los riesgos de la manipulación digital y sus impactos en la vida de las personas.

Palabras clave: *deepfakes*, IA, GANs, derechos digitales, habeas data, ciberdelitos, *soft law*, *hard law*

A los soñadores prácticos, a quienes se atreven a construir el futuro y sobre todo a quienes buscan justicia y protección frente al uso indebido de la inteligencia artificial; que esta obra sea un gesto de memoria y dignidad en la era digital.

Agradecimientos

Agradezco a Dios y al gran amor de mi vida, a mi Lolita querida, por ser mi ejemplo y mi fortaleza. Estuviste presente en cada etapa de mi vida, me acogiste como hija y me enseñaste a ser valiente. No me alcanzará la vida para agradecerte todo lo que hiciste y sigues haciendo por mí. Quiero agradecer también a mi querida familia, Carlita, Cris, Rober, Rey, Cristian, Noé, Faby, Jeny, Edid, Patricio, Evelyn, y a los más pequeños, Sebas, Arleth e Isaac su apoyo incondicional y su resiliencia me inspiran a seguir siempre adelante. Gracias de corazón, por tanto.

Agradezco a la Universidad Andina Simón Bolívar - Sede Ecuador y a mi tutor de tesis Juan Mejía por su acompañamiento constante y sus valiosos aportes que guiaron mi investigación. Extiendo mi agradecimiento a Claudia, Cristian, César, Enrique, Luis, Marco, Ramiro, Elsita, Gabriel, María Augusta, Agustín, Sebastián, Fausto, Ximenita y Atahualpa, lo vivido en las aulas y fuera de ellas fue una experiencia profundamente transformadora. Gracias por la importante labor de desarrollar pensamiento crítico, desde el sur de América.

Expreso mi gratitud a mis dos grandes amigos Thalía y Cristian por siempre estar presentes y compartir las alegrías y tristezas de la vida. Agradezco también a mis compañeros de maestría y a todos los maravillosos amigos que esta gran experiencia me permitió conocer Pedro, Andreita, Karen, Carlita, Diani, Stefy, Marita, Jesús, Félix, Walter, Stephano, Alejandro, Javi y Amílcare, gracias por todas las risas y los momentos compartidos. De manera especial extiendo mi agradecimiento a mis amigas Pao, Vane y Claudia por sus invaluables palabras de aliento en este arduo proceso.

Finalmente, muchas gracias a todas las personas que generosamente compartieron su tiempo, sus experiencias y sus historias de vida, para que este trabajo vea la luz, esta obra también es suya y cada página lleva algo de ustedes.

Tabla de contenidos

Figuras y tablas

Siglas

IA Inteligencia artificial

TIC Tecnologías de la información y comunicación

COIP Código Orgánico Integral Penal

CRE Constitución de la República del Ecuador

RIA Reglamento de Inteligencia Artificial

UE Unión Europea

GANs Es el plural de GAN y significa Generative Adversarial Networks. En español se traduce como redes generativas antagónicas y se mantiene la sigla original por su uso extendido en la literatura científica.

Glosario

Inteligencia artificial: En la informática, se trata de un área que busca crear sistemas capaces de imitar procesos propios de la inteligencia humana, como aprender, tomar decisiones propias o adaptarse a nuevas situaciones.

Deepfakes: Los *deepfakes* son contenidos audiovisuales creados mediante inteligencia artificial generativa, que simulan la apariencia, voz o gestos de una persona, que parece real, aunque el contenido sea completamente falso.

***Deepfakes* pornográficos**: Es una variante de los *deepfakes* utilizada para generar contenido sexualmente explícito sin el consentimiento de las personas afectadas, vulnerando su dignidad y derechos fundamentales de la persona.

Tecnologías de la información y comunicación: Son el conjunto de herramientas, recursos y sistemas que permiten crear, almacenar, procesar, transmitir y compartir información de manera digital y eficiente.

Soft law: Se trata de normas no vinculantes, como los principios éticos de la IA y las recomendaciones, que orientan el uso de IA, pero su aplicación no es obligatoria.

Hard law: Son un conjunto de normas jurídicas de cumplimiento obligatorio, que establecen sanciones para la protección de derechos frente a riesgos tecnológicos.

Derechos digitales: Es el conjunto originado a partir del uso del internet y que protegen a las personas en el entorno digital, como privacidad, seguridad y acceso a la información.

Dignidad humana: Es el reconocimiento del valor intrínseco que posee cada persona por el simple hecho de serlo. Este derecho, no depende de logros, condiciones sociales ni capacidades físicas o mentales, es inherente, irrenunciable e inalienable

Derecho a la intimidad: Se trata de un derecho fundamental que protege la esfera íntima de la persona, permitiéndole vivir con dignidad y sin intromisiones arbitrarias.

Derecho a la integridad: Es un derecho humano fundamental que protege la totalidad del ser humano en sus dimensiones física, psíquica, moral y sexual, garantizando que ninguna persona sea sometida a violencia, tratos crueles o humillantes

Derecho de indemnidad sexual: Es el derecho de niñas, niños, adolescentes y personas con discapacidad, a no sufrir interferencias en la formación de su sexualidad.

Introducción

El presente estudio se basa en analizar el impacto de los *deepfakes* pornográficos en los derechos de las personas, cuyo planteamiento se justifica en el avance que ha tenido la inteligencia artificial (en adelante IA), en los múltiples sectores de la sociedad, a través de herramientas tecnológicas capaces de transformar la forma de interacción social en el entorno virtual y la realidad social. Las creaciones artificiales como los *deepfakes* han surgido como una de las aplicaciones más sofisticadas y controversiales de la IA, permitiendo la manipulación de imágenes y videos con un elevado nivel de realismo. A pesar de que su uso puede ser positivo, en campos como el entretenimiento, la educación y la ciencia, la utilización indebida de esta tecnología ha generado graves preocupaciones sociales y jurídicas.

Uno de los problemas más graves derivados de los *deepfakes* es su uso en la creación de contenido pornográfico sin consentimiento, lo que afecta directamente la dignidad de las personas involucradas. Este fenómeno evidencia los riesgos que plantea la IA cuando se emplea sin una regulación adecuada, convirtiéndose en una herramienta que facilita la vulneración de derechos fundamentales. La difusión de contenido falso ha generado consecuencias en la vida de quienes han sido víctimas de estas prácticas. A partir de esta problemática, la presente investigación propone indagar la manera en que el derecho y la sociedad pueden abordar y responder ante la inminente vulneración de derechos que implica el uso de *deepfakes* pornográficos, especialmente en el contexto social ecuatoriano, en el que la IA aún no ha sido comprendida, ni regulada.

El estudio se estructura en dos capítulos complementarios, el primero se enfoca en analizar el impacto social de los *deepfakes* pornográficos en los derechos de las personas, abordando su origen, la evolución tecnológica, los desafíos éticos y educativos, con el propósito de promover la reflexión crítica. El segundo capítulo, examina los desafíos jurídicos en el contexto ecuatoriano ante la posible regulación de los *deepfakes* pornográficos, evaluando las respuestas actuales desde el *hard law* e iniciando la discusión de una futura regulación en el entorno digital. El análisis de esta problemática se desarrollará mediante un enfoque cualitativo, con carácter descriptivo y deductivo. La técnica empleada será la revisión bibliográfica y documental, lo que permitirá interpretar críticamente el fenómeno desde diferentes enfoques.

Además, se desarrollará un estudio de casos de personas afectadas por este tipo de tecnología, mediante entrevistas construidas bajo el enfoque de historia de vida. La selección de casos se realizará mediante una triangulación cualitativa, que articulará tres métodos de carácter cualitativo. Esta combinación permitirá reconstruir las trayectorias personales en profundidad y comprender el impacto jurídico, social y emocional, que este fenómeno tecnológico ha tenido en la vida de las personas. De la misma manera, se efectuarán entrevistas a especialistas en la temática, para ello se ha empleado el método cualitativo intencional, seleccionando a referentes en cada área jurídica cuya trayectoria y experticia, permiten enriquecer el análisis desde diversas perspectivas.

En el marco del derecho comparado, se desarrollará un análisis general de las legislaciones vigentes en la Unión Europea, China y Estados Unidos, en relación con la regulación de la IA, sus niveles de riesgo y los mecanismos sancionatorios aplicables. Este recorrido permitirá identificar los enfoques normativos predominantes a nivel global, así como establecer el grado de riesgo que representan los *deepfakes* de carácter pornográfico en dichos sistemas jurídicos. Por otra parte, aunque en América Latina la legislación sobre la IA y los *deepfakes*, aún se encuentra en una fase de desarrollo, se examinará la normativa de Brasil, México, Colombia y Ecuador, con especial atención a los marcos de protección de datos personales, los delitos digitales y los proyectos legislativos emergentes vinculados al desarrollo de tecnologías disruptivas como la IA y sus creaciones sintéticas.

Finalmente, se desarrollará un análisis de la legislación interna ecuatoriana en sus distintas ramas del derecho, con el propósito de identificar los vacíos normativos y las tensiones jurídicas que emergen ante el uso indebido de la inteligencia artificial. En este marco, se planteará la necesidad de una futura regulación que visibilice las vulneraciones a los derechos fundamentales derivadas de la aplicación irresponsable de estas tecnologías emergentes. Por todo lo expuesto, esta investigación aspira a generar espacios de diálogo crítico y reflexión interdisciplinaria, orientados a la construcción de soluciones éticas, jurídicas y sociales frente a este fenómeno. Asimismo, busca contribuir a la conformación de una sociedad más consciente, que reconozca los riesgos inherentes al uso de las nuevas tecnologías y sea capaz de enfrentar con responsabilidad los desafíos que plantea la actual realidad digital.

Capítulo primero
Los *deepfakes* pornográficos en la era digital

El mundo se está convirtiendo en una caverna,
igual que la de Platón: todos mirando
imágenes y creyendo que son la realidad.
José Saramago

1. Introducción al fenómeno de los *deepfakes* pornográficos

La investigación pretende dar una mirada introductoria a los *deepfakes*[1] pornográficos, a partir de su origen. Analizando el progreso de este fenómeno hasta su aparición como creaciones digitales que manipulan la veracidad de la información, se plantea una clasificación específica con la finalidad de distinguir los diferentes tipos de *deepfakes* en función de su uso y posible afectación a los derechos. Asimismo, se presenta dos historias de vida cuyos testimonios reflejan el impacto que el mal uso de la tecnología puede generar en la vida de las personas.

La narrativa expone las consecuencias jurídicas y sociales de la utilización maliciosa de las creaciones digitales. El avance en la era digital ha logrado conectar al mundo surgiendo modelos de tecnología cada vez más desarrollados; entre los cuales está la IA. Se trata de un concepto fascinante ya que hace unas décadas era impensable concebir la idea de máquinas inteligentes menos aún capaces de ejecutar tareas humanas, esta concepción solo existía en el imaginario de películas futuristas o literatura de ciencia ficción; hoy en día lo imposible es una realidad.

La tecnología artificial avanza a una velocidad impresionante,[2] influyendo en diferentes ramas del conocimiento tales como, la medicina, la política, la economía, el comercio, etc. En el derecho el avance de la IA ha dado lugar a novedosas formas de práctica judicial, especialmente en materia de juzgamiento. Pero también a posibles

[1] "Los deepfakes son vídeos manipulados donde se suplanta la cara de una persona por la de otra a través de Inteligencia Artificial". Véase en Víctor Cerdán Martínez, María Luisa García Guardia, y Graciela Padilla Castillo, "Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales", *CIC Cuadernos de Información y Comunicación* 2, nº 25 (2020): 1–4, doi:10.5209/ciyc.68762.

[2] Alberto Gil de la Guardia, "Inteligencia Artificial: La Revolución que acelera más rápido que la humanidad puede adaptarse", *sección artículos de LinkedIn*, accedido 2 de septiembre de 2025, párr. 3, https://www.linkedin.com/pulse/inteligencia-artificial-la-revoluci%C3%B3n-que-acelera-m%C3%A1s-alberto-jhxjf/.

vulneraciones de derechos fundamentales[3] y la configuración de ilícitos penales.[4] En el contexto, de la ingeniería social los *deepfakes* están siendo utilizados para detectar vulnerabilidades y generar daños a través de las diferentes plataformas digitales.

La evolución de las tecnologías de la información y la comunicación (en adelante TIC), abarca desde la creación de redes globales como internet, pasando por la integración de la IA, hasta llegar a las creaciones digitales. Se trata de contenido artificial, que puede ser utilizado en contextos científicos, educativos y de entretenimiento; pero también se suele utilizar para desprestigiar la imagen en contextos políticos y reputacionales generando *deepfakes* pornográficos no consentidos,[5] causando daño a la dignidad personal y los derechos fundamentales de la persona.

En las plataformas digitales el 96% de contenido se trata de creaciones explícitas detectadas como no autorizadas,[6] el aumento de contenido malicioso creado mediante IA genera la necesidad de realizar un estudio exhaustivo que permita comprender el fenómeno en su complejidad a partir de sus causas, mecanismos de difusión y los posibles impactos que produce en los derechos de las personas. Asimismo, resulta importante explorar la forma en que incide la ética, la educación digital y la regulación vigente, frente a esta nueva forma de violencia digital.

1.1. Los *deepfakes*: su origen y clasificación

El término *deepfake,* se utiliza para describir contenido generado artificialmente, mediante el modelo de aprendizaje *deep learning*[7] y se puede definir como:

---

[3] Los derechos fundamentales son los reconocidos en la Constitución, en la misma se establece un amplio catálogo de derechos fundamentales. La dignidad y el libre desarrollo se proyectan sobre los derechos constitucionales, al tiempo que su alcance queda delimitado por lo previsto por el constituyente al articular dichos derechos. Miguel Ángel Presno Linera, *Derechos fundamentales e inteligencia artificial* (Madrid: Marcial Pons, 2022), 103.

[4] Leonel Benítez, "Delitos en la era digital", *Revista Pensamiento Penal* 15, nº 24 (2024): 3, https://n9.cl/7o1f6.

[5] "[E]ntre 2022 y 2023, la cantidad de pornografía deepfake creada aumentó un 464%, pasando de 3725 vídeos en 2022 a 21.019 en 2023, un patrón alarmante según los propios investigadores del informe". Véase en Núria Bigas Fortmajé, "Deepfake pornográficos", *Universitat Oberta de Catalunya (UOC)*, accedido 11 de julio de 2025, párr. 2, https://www.uoc.edu/es/news/2023/265-deepfakes-pornograficos-cuando-IA-desnuda-tu-intimidad-vulnera-tus-derechos.

[6] Ximena Córdova, "El aumento de los deepfakes criminales: fraude, pornografía y suplantación de identidad", *Diario El Imparcial*, accedido 31 de agosto de 2025, párr. 5, https://www.elimparcial.com/tecnologia/2024/10/04/el-aumento-de-los-deepfakes-criminales-fraude-pornografia-y-suplantacion-de-identidad/.

[7] "Deep learning is one of the techniques used in machine learning. Deep learning works on the principle of extracting features from the raw data by using multiple layers for identifying different aspects relevant to input data. Deep learning techniques include convolutional network, recurrent neural network, and deep neural network. Deep learning uses artificial neural network, especially the convolutional network". Véase en Ranjan Kumar Mishra, Sandesh Reddy, y Himanshu Pathak, "The Understanding of

> Bajo el término *deepfake* se incluye toda tecnología basada en sistemas de aprendizaje profundo capaz de crear material audiovisual hiperrealista, donde resulta muy difícil, sino imposible, detectar su carácter mendaz. El vocablo *deepfake* está formado por la combinación de los términos *deep* y *fake*. El primero significa profundo, mientras que *fake* se traduce como falsedad o simulación (y sirve en este contexto para describir algo que no es genuino o auténtico).[8]

El *deepfake* es concebido como creación artificial, implica la generación de contenido tecnológico avanzado[9] y también una forma de simulación audiovisual generada a través de la IA generativa, que desafía la percepción de lo auténtico. La profundidad y la falsedad son dos conceptos interesantes pues mientras más sofisticada es la técnica, mayor es el engaño y al ser generadas a través de tecnología artificial, se trata de réplicas tan exactas, cuyo resultado resulta difícil reconocer como falso o generado de manera sintética.

Los *deepfakes* de redes generativas antagónicas (en adelante GANs) mismas que, "Consisten en dos redes neuronales que compiten entre sí: una red generadora y una red discriminadora. El trabajo conjunto de estas redes permite que los deepfakes sean cada vez más realistas".[10] La red generadora crea contenido falso imitando gestos, voces y expresiones reales. El discriminador, lo examina buscando errores; cada corrección que realiza la red discriminadora mejora los detalles hasta que logra engañar a la discriminadora y de esa manera se crean los *deepfakes.*

Las imágenes falsas fueron creadas en 1990,[11] cuando "[L]os investigadores utilizaron CGI para crear imágenes realistas de humanos. Esta tecnología impulsada en

---

Deep Learning: A Comprehensive Review", *Mathematical Problems in Engineering* 5, nº 1 (2021): 2, doi:10.1155/2021/5548884.

[8] Marco Teijón Alcalá, "El deepfake pornográfico: concepto y alcance penal", *Anuario de la Facultad de Derecho de la Universidad de Alcalá* 7, nº 17 (2024): 120–21, doi:10.14679/3901.

[9] "Cuando hablamos de Digital Content o contenido digital en español, nos referimos a todo tipo de información, ya sea educativa, profesional o de entretenimiento, presentada en formato electrónico a través de videos, fotos, presentaciones, audios, artículos web, entre otros". Gonzalo Castillo, "Qué es Digital Content: tipos, funciones y ejemplos", *InnovaciónDigital360*, accedido 2 de septiembre de 2025, párr. 1, https://www.innovaciondigital360.com/industria-4-0/que-es-digital-content-tipos-funciones-y-ejemplos/.

[10] GIRHA TEC, "GANs: La Tecnología Revolucionaria Detrás de los Deepfakes", *GIRHA TEC*, accedido 20 de julio de 2025, párr. 2, https://www.girha.com/blog/gans-la-tecnologia-revolucionaria-detras-de-los-deepfakes.

[11] "La manipulación de fotografías (en el sentido amplio de hacer cambios a la imagen original) existe desde el advenimiento de la técnica fotográfica. […] Adobe Photoshop, lanzado comercialmente en 1990, se convirtió pronto en el programa por excelencia de los profesionales de la imagen, aunque hoy también existen softwares libres muy completos como GIMP (GNU Image Manipulation Program)". Véase en Elke Koppen Prubmann, "Photoforensics y el análisis de imágenes digitales", en *La fotografía en el contexto del cambio: retos y perspectivas*, ed. Héctor Guillermo Alfaro López y Graciela Leticia Raya Alonso (Ciudad de México, UNAM: Universidad Nacional Autónoma de México, 2019), 71.

la década de 2010".[12] Los bocetos de las imágenes eran insertados en la memoria del ordenador, el programa aportaba movimientos en diferentes ángulos, simulando la piel y los músculos para parecer cada vez más natural a medida que avanza la tecnología. El primer *deepfake* tiene su origen en 2017, cuando:

> [G]racias al usuario "deepfakes" desde el programa deepfakes en Reddit en el que compartía videos pornográficos donde insertaba rostros de actrices célebres en cuerpos de actrices porno. Del mismo modo, compartió un código abierto para deep learning en bibliotecas populares y así comenzaron a proliferar deepnudes de manera ilegal en diversos sitios.[13]

Los primeros *deepfakes* pornográficos, afectaron a celebridades como Scarlett Johansson, Taylor Swift, Emma Watson, víctimas de un usuario identificado como *deepfakes* en la plataforma Reddit, quien difundió imágenes íntimas falsificadas de las actrices a través de la red social Twitter hoy en día X. Aunque inicialmente los *deepfakes* fueron contenidos dañinos, su uso se extiende a ámbitos sociales, culturales y científicos. Las categorías se organizan de acuerdo con el medio manipulado, el propósito, el ámbito de circulación, la difusión y la técnica empleada para su creación.

Figura 1. Captura de pantalla de un video deepfake en donde el rostro de una actriz de contenido para adultos es remplazado por el de Taylor Swift, 2022
Fuente: Imagen de Diario El Universo[14]

A continuación, se ofrece una posible clasificación y los derechos afectados:

[12] Gabe Regan, "Una breve historia de Deepfakes", *Reality Defender*, accedido 8 de junio de 2025, párr. 3, https://n9.cl/nyk8d.

[13] Jacob Bañuelos Capistrán, "Evolución del Deepfake: campos semánticos y géneros discursivos 2017-2021", *Revista ICONO 14. Revista científica de Comunicación y Tecnologías emergentes* 20, nº 1 (2022): 11, doi:10.7195/ri14.v20i1.1773.

[14] Redacción EFE, "Los deepfakes, creaciones digitales usadas para perjudicar a mujeres con videos pornográficos falsos", *El Universo*, accedido 14 de octubre de 2025, https://acortar.link/YVwJbC.

Tabla 1
Clasificación de los *deepfakes*

Tipo	Clase	Ejemplos	Posibles derechos afectados a través del mal uso
Según el tipo de contenido	Visual	*Deepfakes de* imagen y vídeo	Dignidad personal Imagen e Identidad personal Honor y Buen nombre Indemnidad Identidad (voz rasgo distintivo) Libertad de expresión (dimensión negativa) Derechos de propiedad intelectual
	Audio	Alteración y clonación de voz	
	Texto	Imitativo o narrativo	
Según el ámbito de circulación y difusión	Público	Redes sociales, amplia difusión; de figuras públicas o particulares.	Imagen personal Protección de datos personales Consentimiento Igualdad y no Discriminación Dignidad humana Integridad psíquica Intimidad y Privacidad
	Privado	Circulan en entornos cerrados a través de mensajería Personas particulares	
Según su finalidad	Benignos	Entretenimiento Educativo Investigación	Por su carácter benigno no afecta, pero debe respetarse los derechos correspondientes a los datos personales, y el consentimiento.
	Maliciosos	Electorales Pornográficos	Participación política Información veraz Honor y reputación Dignidad humana
Según la técnica utilizada	Redes generativas antagónicas (GANs)	Intercambio de rostros Reconstrucción facial	Imagen e identidad personal Intimidad y privacidad Autodeterminación digital Transparencia y veracidad
	Arquitectura Transformer	Crean composiciones visuales altamente realistas	

Fuente: Antonio Fernández et al.[15] y Fernando Ramos Zaga[16]
Elaboración propia

Los *deepfakes* según su contenido se pueden clasificar en "*Deepfaces, deepvoices* y *deep faketext*",[17] mediante los *deepfaces* se modifica imágenes mediante algoritmos de

[15] Antonio Fernández et al., *Deepfakes: Riesgos, Casos Reales y Desafíos en la Era de la IA* (Madrid: Observatorio de Deepfake del ISMS Forum, 2025), https://acortar.link/lFV2hM.

[16] Fernando Ramos-Zaga, "Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial", *Derecho Global. Estudios sobre Derecho y Justicia* 9, nº 27 (2024): 359-87, doi:10.32870/dgedj.v9i27.754.

[17] Fernández et al., *Deepfakes: Riesgos y Desafíos*, 9–15.

aprendizaje profundo, generando rostros que parecen genuinos. En los *deepfaces* se altera el rostro y las gesticulaciones de la persona que se reproducen en las distintas grabaciones haciendo que parezca reales. Del mismo modo, los *deep voices,* se centran en replicar la voz y las gesticulaciones labiales, para que aparente haber dicho cosas que en realidad nunca expresó.

Mediante los *deep faketext* se puede generar escritos en nombre de alguien más, al combinar estas creaciones digitales se produce el *deepfake multimodal,*[18] y al ser mal utilizados pueden llegar a vulnerar derechos fundamentales como la imagen o los derechos de propiedad intelectual. El impacto depende del uso, utilizados de forma responsable pueden ser beneficiosos como el "Entretenimiento para mejorar la calidad de los efectos visuales, doblar actores en diferentes idiomas",[19] e inclusive recrear a personajes famosos, como se hizo con Skywalker un personaje de Star Wars.

En la educación puede generar resultados positivos, ya que "Muchas personas aprenden de forma muy visual, y ver a una persona cobrar vida puede hacer que la experiencia sea aún más especial. […] Un ejemplo de ello es el Museo Dalí, que creó una serie de vídeos de Salvador Dalí hablando con sus visitantes",[20] enriqueciendo el proceso de aprendizaje artístico. Los *deepfakes* han sido utilizados en el entretenimiento y la educación, sin causar perjuicios a la persona. Sin embargo, se debe brindar la protección necesaria a los derechos de autor[21] y los datos personales.

En el contexto ecuatoriano los *deepfakes* de entretenimiento se puede relacionar con la parodia[22] que se trata de una excepción legítima al derecho de autor siempre que

[18] "By combining visual and audio features, our multimodal approach addresses the limitations of unimodal systems, ensuring comprehensive feature extraction and robust detection. This method demonstrates superior accuracy and reliability, making it a significant advancement in the field of deepfake detection". Kashish Gandhi et al., "A Multimodal Framework for Deepfake Detection", *Journal of Electrical Systems* 20, nº 10 (2024): 85, https://journal.esrgroups.org/jes/article/view/6126.

[19] The Black Box Lab, "Deepfakes: La Realidad Transformada, Tipos y Aplicaciones", *The Black Box Lab*, accedido 2 de septiembre de 2025, párr. 5, https://theblackboxlab.com/deepfakes/.

[20] "Many people are very visual learners, and seeing a person come to life can really make the experience even more special. [...] One example of this is the Dalí Museum, which created a series of videos of Salvador Dalí speaking with its visitors". Bryan Lyon y Matt Tora, *Exploring Deepfakes* (Birmingham: Packt Publishing, 2023), 35–8.

[21] Los derechos de autor, se pueden definir como una vía de protección a las obras literarias, artísticas y científicas que forma parte del derecho genérico de la propiedad intelectual, que no necesitan registro y nacen a partir de que la obra es creada. Véase en Sergio Mondragón Duarte et al., "Protección jurídica de los derechos de autor en Colombia", *SUMMA. Revista disciplinaria en ciencias económicas y sociales* 4, nº 1 (2022): 3–6, doi:10.47666/summa.4.1.09.

[22] La sátira, pastiche o parodia de una obra divulgada, siempre que se ajuste a las reglas de estos géneros, mientras no implique el riesgo de confusión con ésta, ni ocasione daño a la obra o a la reputación del autor o del artista intérprete o ejecutante, según el caso. En ningún caso esta utilización podrá constituir una explotación encubierta de la obra. Ecuador, *Código Orgánico de la Economía Social de los Conocimientos,* Registro Oficial, Suplemento 889, 9 de diciembre de 2016, art. 212 núm. 13.

mantenga un carácter humorístico que sea justificable y que además respete las normas en cuanto a obras protegidas.[23] En el caso de los *deepfakes*, existe una complejidad pues además de utilizar obras protegidas, incorporan la imagen, la voz y otros rasgos de identidad personal generando una intersección entre derechos de la personalidad[24] y derechos de autor.

Se puede considerar que los *deepfakes* benignos son creados con fines humorísticos, paródicos o educativos cuando reflejan la creatividad digital que busca provocar risa, reflexión o aprendizaje, siempre que se respete el consentimiento y las normas de protección de datos. En ese sentido, los derechos de autor no sólo garantizan el respeto a la reproducción de obras ajenas, sino que también sirven para establecer si un *deepfake* puede ser reconocido como una parodia legítima o, por el contrario, constituye una infracción.

Los *deepfakes* al ser utilizados de manera maliciosa pueden causar daño o terminar en la consumación de actos delictivos, generando consecuencias graves a la dignidad y los derechos conexos de la persona. Actualmente, "Los principales campos discursivos del deepfake están en la esfera de la política y la pornografía",[25] en los cuales podría generarse daños como el desprestigio, la usurpación de identidad para sortear sistemas de seguridad biométrica inclusive delitos más graves como la segmentación y ataques a comunidades, pueblos o nacionalidades.

Los videos sexuales falsos, difundidos a través de las redes sociales como los *deepfakes* pornográficos han afectado a celebridades y al pasar del tiempo los *ultrafalsos*[26] no sólo han perfeccionado su realismo técnico, sino también han amplificado su alcance hacía personas particulares que se encuentran fuera del foco mediático.

---

[23] "La protección reconocida por el presente Título recae sobre todas las obras literarias, artísticas y científicas, que sean originales y que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocerse". Ibíd., art. 104.

[24] "Son derechos subjetivos constituidos por un haz unitario de facultades cuyo ejercicio y defensa se encomienda a su titular, son predicables, propiamente y sólo, de los bienes sociales e individuales". Carlos Rogel Vide, "Origen y actualidad de los derechos de la personalidad", *REVISTA IUS* 1, nº 20 (2017): 7-10, doi:10.35487/rius. v1i20.2007.278.

[25] Jacob Bañuelos Capistrán, "Deepfake: la imagen en tiempos de la posverdad.", *Revista Panamericana de Comunicación* 2, nº 1 (2020): 5, doi:10.21555/rpc. v0i1.2315.

[26] "Los deepfakes (también llamados 'ultrafalsos' o 'ultrafalsificaciones' en español) se refieren a imágenes, vídeos, clips de audio u otros creados mediante aprendizaje profundo (deep learning, un subcampo de la inteligencia artificial o IA) en los que el contenido se altera con resultados hiperrealistas para que parezca que las personas hicieron o dijeron cosas que realmente no sucedieron o nunca dijeron". Michelle Azuaje Pirela, "Deepfakes, distorsión de la realidad y desafíos jurídicos", *Telos Fundación Teléfonica*, accedido 2 de septiembre de 2025, párr. 3, https://telos.fundaciontelefonica.com/telos-122-posverdad-regulacion-michelle-azuaje-deepfakes-distorsion-de-la-realidad-y-desafios-juridicos/.

Finalmente, en la creación de *deepfakes* se utilizan diversas técnicas que replican contenido hasta lograr una alta similitud con el original, como, por ejemplo:

> Las GAN son modelos generativos no supervisados que localizan automáticamente la distribución de datos. El «generador» y el «discriminador» son los dos modelos principales de un sistema GAN. Un tipo de red neuronal, la red convolucional, se encarga de generar datos, mientras que otro tipo de red, la red deconvolucional, se utiliza para la clasificación.[27]

Las GANs son dos redes complementarias, una es denominada generadora mediante la cual se ingresa el contenido auténtico y el contenido falso para que pueda producir la creación digital, una vez realizada el producto es analizado por la red discriminadora la cual determina si este contenido es real o falso, al determinar que es falso nuevamente inicia el proceso para que la red generadora perfeccione el contenido, por tanto ambas redes trabajan de manera complementaria hasta que la red generadora logra validar el contenido como real ante la red discriminadora.

Una nueva forma de generar *deepfakes* es mediante la arquitectura Transformer introducida en el año 2017, a través del artículo *Attention Is All You Need,*[28] basada en modelos de autoatención[29] se puede definir como, "Una nueva arquitectura que destaca por usar mecanismos de atención, además de ofrecer capacidad para paralelizar tareas".[30] Estas redes se encargan de procesar texto, audio e imágenes, con una calidad sorprendentemente alta, cada red se encarga de una parte denominada *parche;*[31] está

---

[27] "The GANs are unsupervised generative models that automatically locate the data distribution. The 'Generator' and the 'Discriminator' are the two main models in a GAN system. One type of neural network, a convolutional network, is responsible for generating data, while another type of network, a deconvolution network, is used for classification". Preeti Sharma et al., "Generative adversarial networks (GANs): Introduction, Taxonomy, Variants, Limitations, and Applications", *Multimedia Tools and Applications* 83, nº 41 (2024): 2–3, doi:10.1007/s11042-024-18767-y.

[28] Roberto Crespo, "Transformer: Attention is all you need", *Tecnología, marketing digital y desarrollo personal*, accedido 24 de agosto de 2025, párr.5, https://www.robertocrespo.net/transformer-attention-is-all-you-need/.

[29] "La autoatención es un mecanismo que permite a un modelo sopesar la importancia de los distintos elementos de una misma secuencia de entrada. En lugar de tratar cada parte de la entrada por igual, permite al modelo centrarse selectivamente en las partes más relevantes al procesar un elemento específico. Esta capacidad es crucial para comprender el contexto, las dependencias a largo plazo y las relaciones dentro de los datos, y constituye la base de muchas arquitecturas modernas de Inteligencia Artificial (IA), en particular el Transformador". Ultralytics, "La autoatención explicada", *Ultralytics*, accedido 2 de septiembre de 2025, párr.1, https://www.ultralytics.com/es/glossary/self-attention.

[30] Crespo, "Transformer: Attention is all you need", párr. 3.

[31] "Vision Transformer opera dividiendo la imagen de entrada en una cuadrícula de parches de imágenes, tratando cada parche como un token similar a las palabras en una oración. Estos tokens se incrustan junto con incrustaciones de posición para retener información espacial, un componente crucial para entender la imagen en su totalidad". Koen De Jong, "El poder de ViT, Transformadores de Visión para el Reconocimiento de Imágenes", *Visionplatform.ia*, accedido 25 de agosto de 2025, párr.2, https://acortar.link/vhakyW.

técnica mantiene los trazos sin romper la armonía visual y se la denomina autoatención siendo la base de la arquitectura Transformer.

La siguiente gráfica muestra las aplicaciones basadas en GANs y Transformers:

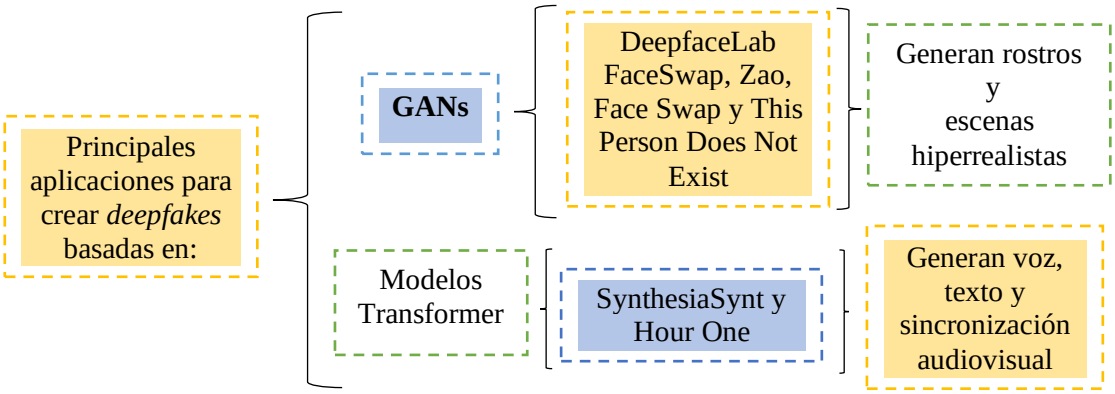


Figura 2. Aplicaciones de *deepfakes*, Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad, 2021
Fuente: Adaptado de Juan Boté y Mari Vállez[32]

Las aplicaciones para la creación de *deepfakes* en base a GANs, como DeepfaceLab FaceSwap, FaceSwap, Reface, Zao y This Person Does Not Exist, permiten generar imágenes y videos sintéticos hiperrealistas, debido a ello surgen riesgos como la suplantación de identidad, el desprestigio, la violencia simbólica y desinformación. Los modelos Transformers como SynthesiaSynt y Hour One, generan voz, texto y sincronización visual, pero cuando se emplean de forma inapropiada, pueden representar un riesgo elevado, para la imagen y veracidad de la información.

1.2. Siglo XXI: evolución de las TIC a la generación de *deepfakes*

En este apartado se analizará la evolución de las TIC, hasta el desarrollo de la IA y sus nuevas creaciones digitales. La IA ha evolucionado desde enormes máquinas, circuitos y microchips; llegando a convertirse en una de las tecnologías más debatidas y controversiales del periodo contemporáneo. El impacto ha sido tan profundo al punto de volverse parte de la vida cotidiana; es impensable hoy en día no convivir con la tecnología. Los dispositivos digitales como el *smartphone* u ordenadores portátiles ofrecen una amplia gama de servicios y aplicaciones, que facilitan tareas cotidianas.

Para analizar la evolución de las TIC, es preciso dividirlo en tres etapas, la primera se denomina los inicios del desarrollo tecnológico, seguidamente la era de la computación

[32] Juan José Boté Vericad y Mari Vállez, "Aplicaciones de deepfakes. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad", *Documentación de las Ciencias de la Información* 45, nº 1 (2022): 25–32, doi:10.5209/dcin.77256.

y finalmente la revolución digital.[33] La evolución tecnológica ha cambiado la forma en que las personas interactúan y obtienen información. Las TIC, como se denominan, tuvieron sus inicios en inventos como la escritura y el cálculo. La escritura surgió como un medio para registrar la vida cotidiana,[34] sin imaginar que serviría para la creación de nuevos inventos como la imprenta y posteriormente el telégrafo.

A lo largo del tiempo, se ha logrado compilar el conocimiento humano; transmitiéndolo de una generación a otra. Los datos recopilados son un precedente y fuente de información para los medios digitales.[35] Los estudios de cálculo diferencial[36] realizados por Newton y Leibniz, fueron trascendentes, dado que ambos coincidieron "En muchas de las premisas más importantes del cálculo de manera independiente".[37] Si bien no existían los avances tecnológicos actuales, el cálculo inició las bases para el desarrollo de los algoritmos modernos utilizados en IA generativa.

La segunda etapa de evolución de las TIC inicia con la primera computadora que durante años intentó construir Charles Babbage.[38] Aunque su construcción no logró concretarse, constituyó un avance en el desarrollo de la tecnología, pues se trataba de una gran memoria capaz realizar operaciones aritméticas complejas. Más adelante, la científica y programadora Ada Lovelace, "[S]e interesó en el trabajo de Babbage e ideó un programa de *software* para solventar diversos problemas de programación de la maquina analítica".[39] La visión de la máquina analítica de Babbage y las contribuciones de Lovelace, marcaron el precedente para el futuro desarrollo de la tecnología digital.

La primera computadora electrónica, fue "La ENIAC, presentada en 1945, una máquina colosal que pesaba casi 35 toneladas y ocupaba un espacio de 167 metros

---

[33] Ignasi Belda, *Inteligencia Artificial*, Primera (Barcelona: RBA Coleccionables, S. A., 2019), 14-20.

[34] Yandry Jesús Espinoza Andrade et al., "Evolución del Manejo de las TIC en la Informática y su Impacto en el Uso de Recursos Informáticos", *Ciencia Latina Revista Científica Multidisciplinar* 8, nº 4 (2024): 3-4, doi:10.37811/cl_rcm. v8i4.12482.

[35] Antonio García Jiménez y Beatriz Catalina García, "Una perspectiva documental y bibliotecológica sobre el big data y el periodismo de datos", *Investigación Bibliotecológica: archivonomía, bibliotecología e información* 32, nº 74 (2018): 2, doi:10.22201/iibi.24488321xe.2018.74.57910.

[36] "El cálculo diferencial investiga las propiedades de las razones de cambio comparativas de variables que están vinculadas por medio de ecuaciones. [...] Resulta que cuando se usa la intuición para pensar en ciertos fenómenos —movimiento de los cuerpos, cambios en la temperatura, crecimiento de poblaciones y muchos otros—, se llega a postular ciertas relaciones entre estas variables y sus razones de cambio. Estas relaciones se escriben en una forma conocida como ecuaciones diferenciales". Dennis Zill y Warren Wright, *Matemáticas 1: cálculo diferencial* (Ciudad de México: McGraw-Hill Interamericana Editores, 2011), 20-8.

[37] Ibíd., 174.

[38] Miguel Camacho, "Historia y Computación: Estudiar el pasado con los medios más modernos", *Historia y Espacio* 2, nº 15 (2018): 5, doi:10.25100/hye. v0i15.6886.

[39] Belda, *De los circuitos a las máquinas pensantes*, 30-34.

cuadrados".[40] La misma se basó en el desarrollo del lenguaje de programación, los procesos lógicos y el almacenamiento de información binaria. En 1943, McCulloch y Pitts "Propusieron un modelo de computación completamente inspirado en el funcionamiento de las neuronas biológicas",[41] siendo la primera vez que la tecnología se basó en las bases cognitivas para su desarrollo.

Paralelamente, en el año de 1950 Alan Turing concibe por primera vez la idea de una IA, el matemático "Presentó un test basado en una idea muy simple: si una máquina se comporta en todos los aspectos como un ente inteligente, entonces es que debe de ser inteligente".[42] Turing, actualmente reconocido como el padre de la IA, tras descifrar el código enigma[43] creó un legado perdurable en la informática, se trata del célebre *Test de Turing*,[44] que constaba de un cuestionario de preguntas y respuestas previamente estructurado para distinguir si una entidad es inteligente.

En la era de la IA, conocer este test, así como sus variantes, resulta fundamental para determinar posibles engaños generados a través de la tecnología y el contenido digital. Tras la formulación de este test, en el año de1956 se celebró el famoso *Dartmouth Workshop*,[45] en cuyo evento inicia el nacimiento oficial de la IA como disciplina formal. En las décadas posteriores, la IA experimentó etapas de crecimiento y deceso, denominadas como inviernos de la IA,[46] cuando el interés en el desarrollo tecnológico se redujo por falta de financiación y desarrollos técnicos suficientes.

---

[40] "The ENIAC, unveiled in 1945, a colossal machine that, [...] weighed almost 35 tons and occupied a space of 167 square meters". Alan Duncan Gilchrist, "From Punched Cards to Google: An Outline History of Information Retrieval", *Scire: Representación y Organización Del Conocimiento* 24, nº 1 (2018): 2, doi:10.54886/scire. v24i1.4598.

[41] Rubén Rodríguez Abril, "Neuronas de McCulloch y Pitts Artículo de LMO", *La Máquina Oráculo*, accedido 19 de mayo de 2025, párr. 3, https://lamaquinaoraculo.com/deep-learning/el-modelo-neuronal-de-mcculloch-y-pitts/.

[42] Belda, *De los circuitos a las máquinas pensantes*, 37-40.

[43]"La máquina Enigma cifraba mensajes mediante permutaciones reversibles llamadas 'involuciones', donde cada letra se transformaba en otra y podía volver a su forma original. Como el proceso de cifrado y descifrado era idéntico, bastaba con que ambas partes compartieran la misma configuración, que actuaba como clave secreta. Enigma funcionaba como un candado que cambiaba cada día, y solo quienes conocían la combinación podían revelar el mensaje oculto". Guillermo Morales Luna, "La criptología y la victoria aliada en la Segunda Guerra Mundial", *Revista Ciencia* 64, nº 4 (2013): 3, doi: 10.25186/rev.ciencia.2013.4.6886.

[44] "The Turing test is an operational test; that is, it provides a concrete way to determine whether the entity is intelligent. The test involves a human interrogator who is in one room, another human being in a second room, and an artificial entity in a third room". Richard Napolitan y Xia Jiang, *Artificial Intelligence with an Introduction to Machine Learning* (New York: Taylor & Francis Group, 2018), 24-30.

[45] "Algunos hitos importantes refieren que desde1956 es cuando se habla por primera vez del término IA en un congreso en Dartmouth". José Ramón Sanabria Navarro et al., "Incidencias de la inteligencia artificial en la educación contemporánea", *Comunicar* 31, nº 77 (2023): 8, doi:10.3916/C77-2023-08.

[46] "Los investigadores en Inteligencia Artificial se encontraron con limitaciones y dificultades insalvables en la década de los 70. La escasa capacidad de computación de las máquinas impedía procesar

A partir de 1990, inicio el aprendizaje automático o *machine learning*, definido como, "[E]l campo de estudio que da a los computadores la capacidad de aprender sin ser programados de manera explícita".[47] Al principio, las computadoras ejecutaban tareas mediante la programación tradicional o manual, lo que implicaba una dependencia del programador humano, con el desarrollo del aprendizaje automático los programas empezaron a realizar tareas de manera autónoma, a través del entrenamiento previo de algoritmos, sin requerir la intervención directa del desarrollador.

Posteriormente, surgió el *deep learning* o aprendizaje profundo, así:

> "Científicos como Geoffrey Hinton comenzaron a esbozar un modelo de IA ahora llamado aprendizaje profundo que imitaba estructuralmente al cerebro humano. Este proceso es un ejemplo del campo más amplio llamado aprendizaje automático (Machine learning, ML en inglés), y cuando escuchamos la frase IA, a lo que la gente generalmente se refiere es a varias técnicas de aprendizaje automático como las redes neuronales de aprendizaje profundo, el aprendizaje de refuerzo o la inferencia bayesiana. El ML puede ser un subconjunto de la IA, pero hoy en día es el más importante."[48]

El *deep learning* constituye una subcategoría del aprendizaje automático, caracterizado por el uso de redes neuronales artificiales que buscan emular, de manera estructural el funcionamiento del cerebro humano. Estas redes detectan patrones complejos en grandes conjuntos de datos y permiten que el sistema aprenda de manera autónoma sin una instrucción especifica. La arquitectura del aprendizaje profundo se inspira en la neurobiología, pero más que una reproducción cognición, se trata de un funcionamiento basado en principios estadísticos e informáticos.

Finalmente, los "[A]vances en el tamaño y la velocidad de los modelos de aprendizaje profundo han sido catalizadores clave en el desarrollo de innovaciones en inteligencia artificial generativa".[49] Siendo la base para la creación de nuevos contenidos digitales e impulsados por los modelos de aprendizaje profundo como las GANs,[50]

---

grandes cantidades de datos, algo indispensable para entrenar modelos complejos". Nuria Oliver, *INTELIGENCIA ARTIFICIAL* (Madrid: Ministerio de Asuntos Económicos y Transformación Digital, 2021), 40-44.

[47] Jorge Díaz Ramírez, "Aprendizaje Automático y Aprendizaje Profundo", *Ingeniare. Revista chilena de ingeniería* 29, nº 2 (2021): 2, doi:10.4067/S0718-33052021000200180.

[48] Michael Bhaskar y Camila Rocca, "La Inteligencia Artificial y las editoriales", *Trama Editorial* 12, nº 44 (2025): 4, doi:190.216.103.250.

[49] Decide Soluciones, "IA Generativa: qué es, historia, tipos y casos de uso", *Decide Soluciones*, accedido 3 de septiembre de 2025, párr. 3, https://decidesoluciones.es/ia-generativa-que-es-historia-tipos-y-casos-de-uso/.

[50] "Generative Adversarial Networks, or GANs for short, are an approach to generative modeling using deep learning methods, […] are a clever way of training a generative model by framing the problem as a supervised learning problem with two submodels: the generator model that we train to generate new examples, and the discriminator model that tries to classify examples as either real". Jason Brownlee, *Generative Adversarial Networks with Python* (Melbourne: Machine Learning Mastery, 2021), 35-42.

propuestas en el año 2014 por Ian Goodfellow, para la creación de contenido artificial, que resultó ser impresionantemente realista, o los Autocodificadores Variacionales (VAEs) y más recientemente la arquitectura Transformer.

2. *Deepfakes* pornográficos: violencia digital en la realidad contemporánea

La violencia digital se puede definir como "[T]oda acción dolosa basada en difundir o transmitir imágenes, audio y vídeos con contenido sexual íntimo, causando daño a la privacidad y la dignidad de la persona".[51] Se trata de una forma grave de vulneración de los derechos de la persona, utilizando su imagen como medio para causar daño, cuya característica fundamental de esta violencia es el uso de las TIC; para crear y difundir contenido de carácter sexual.

Por otro lado, para efectos de esta investigación se entenderá el concepto de pornografía según lo ha definido la Real Academia Española como, "Modo de presentar el sexo abiertamente y con crudeza, para producir excitación".[52] El contenido pornográfico *online* constituye un medio audiovisual o gráfico, que representa actos sexuales o de desnudez con fines de excitación, y se distribuye a través de internet. Se puede incluir videos, imágenes, textos, animaciones o transmisiones en vivo, y está disponible en múltiples plataformas, tanto gratuitas como de pago.

Los *deepfakes* pornográficos, surgieron como una de las expresiones más alarmantes de violencia digital, se trata de la "Creación de videos falsos, extremadamente realista, en la cual un rostro de una persona, es incrustado en el cuerpo de otra persona realizando una actividad pornográfica"[53] Este tipo de pornografía sintética,[54] se produce mediante las GANs o la arquitectura Transformer, utilizando contenido original en el que

[51] Carmen Carolina Ortega Hernández, Norma Esther López Maldonado, y Teresa Del Carmen Cabrera Gómez, "Violencia digital y afectiva en redes sociales", *Transdigital* 5, nº 10 (2024): 5, doi:10.56162/transdigital374.

[52] RAE, "pornografía", *Real Academia Española*, accedido 18 de septiembre de 2025, párr. 1, https://www.rae.es/diccionario-estudiante/pornografía.

[53] Franklin Geovanny Sinaluisa Sagñay, Wendy Pilar Romero Noboa, y Nelson Francisco Freire, "Deepfakes Pornográficos: Impacto jurídico-probatorio y social en el Ecuador", *Reincisol* 3, nº 6 (2024): 6, doi:10.59282/reincisol. V3(6)2912-2934.

[54] "Un tipo de contenido que se difunde y viraliza rápidamente en la actualidad, afectando a celebridades o personajes públicos como a personas con vidas privadas, así también señalan que los principales derechos vulnerados con los deepfakes pornográficos o sexuales, son la integridad sexual, la identidad personal y la intimidad". Estefany Alvear Tobar y Nicole Enríquez Espinoza, "Tipos penales para conductas que vulneran la integridad sexual, a través del mal uso de inteligencia artificial en Ecuador", *Derecho Penal Central* 5, nº 6 (2025): 9, doi:10.29166/dpc. v6i6.7701.

se reemplaza la cara o el cuerpo de la persona sin su autorización, a cuyo fenómeno se le ha denominado *face swapping*[55] o cambio de caras.

El abogado y especialista en ciberseguridad, Luis Enríquez, señala que "Hace algunos años se puso de moda los *deepfakes*, como una manera de hacer una broma, utilizando imágenes de figuras públicas como Donald Trump o Greta Thunberg",[56] Los primeros *deepfakes*, concebidos inicialmente como ejercicios de entrenamiento técnico e incluso con fines humorísticos, pronto derivaron en aplicaciones de carácter malicioso. Según el especialista, aquello que comenzó como una parodia se transformó en un recurso capaz de afectar gravemente los derechos personales y en ciertos casos de generar conflictos vinculados a la propiedad intelectual.

Estas técnicas se empleaban con fines humorísticos o experimentales, insertando rostros de figuras públicas en escenas ficticias para provocar sorpresa, entretenimiento o reflexión. A pesar de ello su uso podría llegar a vulnerar derechos personales como la honra, la intimidad o la reputación de una persona. Por otro lado, también se relacionan con los derechos de autor cuya excepción es la parodia, que permite transformar obras protegidas con fines humorísticos, críticos o reflexivos, siempre que no se vulneren injustificadamente los derechos del autor.

Según Jorge Climent, en el contexto de los *deepfakes* la parodia se identifica de la siguiente manera:

> El Tribunal de Luxemburgo resolvió que la parodia tiene, por características esenciales, por un lado, evocar una obra existente, si bien diferenciándose perceptiblemente de ésta, y, por otro, plasmar una manifestación humorística o burlesca. Se puede afirmar que los elementos básicos de la parodia son dos: el primero, que la obra sea, a los ojos del espectador, diferenciable de la que toma como referencia, y el segundo que, además, haya una manifestación humorística o burlesca en dicha obra.[57]

Este tribunal ha señalado que la parodia puede evocar una obra existente diferenciándose de ella y contener un elemento humorístico o burlesco, criterio que coincide con el Código Ingenios en Ecuador, donde se admite la parodia como excepción

---

[55] "[E]l face-swapping, cambio de caras en inglés, y la combinación de face-swapping y lip-syncing es, según Sankaranarayanan, el sistema más popular y extendido para elaborar los deepfakes audiovisuales que proliferan en redes sociales". Ignacio Carrascón Vilches Sandra, "¿Qué hace falta para que tus ojos vean algo que nunca ocurrió? Así se crean los 'deepfakes' en vídeo y en imagen", *Newtral*, accedido 16 de mayo de 2025, párr. 13, https://www.newtral.es/deepfakes-audiovisuales/20241022/.

[56] Luis Enríquez, entrevistado por la autora, 25 de julio de 2025. Para leer la entrevista completa, ver Anexo 4.

[57] Jorge Antonio Climent Gallard, "Los deepfakes satíricos o paródicos: análisis desde la perspectiva del derecho europeo", *Revista Boliviana de Derecho* 2, nº 39 (2025): 62, https://www.revista-rbd.com/wp-content/uploads/2025/06/rBD39_Art_02.pdf.

a los derechos de autor si es diferente a la obra original y no afecta injustificadamente al autor. Los *deepfakes* humorísticos pueden considerarse parodia válida siempre que provoquen risa o reflexión sin vulnerar la honra, intimidad o reputación de las personas.

Posteriormente, el experto Luis Enriquez señala lo siguiente:

> [Y]a paso de ser una broma a ser un arma para cometer diversos delitos, incluyendo la creación de pornografía no consentida. Actualmente, ya no se necesita saber programación ni dominar lenguajes como Python, basta con adquirir créditos en plataformas accesibles en línea, subir una imagen o video, y el contenido falso está listo para difundirse.[58]

En la actualidad, no es indispensable poseer conocimientos avanzados en programación para crear contenido digital. Es suficiente, con mantener acceso a internet y contar con un dispositivo móvil o una computadora, para descargar las aplicaciones necesarias, que permitan generar y difundir dicho contenido en las diversas plataformas digitales. La democratización de la tecnología,[59] "Plantea preocupaciones sobre el consentimiento y el control de la imagen".[60] Así es que el debate se ha centrado en el uso de las TIC, cada vez más desarrolladas y cercanas al ciudadano común.

La IA es una herramienta que no tiene una finalidad propia y por tanto depende del ser humano; cuya intención determinará el producto que genera dicha herramienta. En Ecuador, el consentimiento en la generación de contenido digital se define como, "[L]a manifestación de la voluntad libre, específica, informada e inequívoca, por el cual el titular de los datos personales autoriza al responsable a tratar los mismos".[61] La ausencia de consentimiento, se evidencia en la creación de imágenes y videos sexuales generados a partir de material extraído de fuentes públicas como redes sociales.

Esta práctica vulnera la autonomía y es una forma de apropiación digital, facilitada por la creciente accesibilidad a esta tecnología normalizando la generación de los *deepfakes* pornográficos similar a la pornografía de venganza,[62] debido a la falta de

---

[58] Ibíd., Anexo 4.

[59] "El acceso a la tecnología (la democratización de las herramientas de creación) ha permitido que en la actualidad cualquier persona, educada o no en comunicación visual, pueda producir y difundir sus propias imágenes". Isabel Herrera González, "Democratización de la tecnología: emisores contemporáneos", *El Pájaro de Benín* 1, nº 8 (2022): 9, doi:10.12795/pajaro_benin. 2022.i8.05.

[60] Cecilia Barba Arteaga, "Deepfakes sexuales: impacto, prevención y perspectivas de género en el entorno digital", *Miguel Hernández Communication Journal* 15, nº 2 (2024): 9, doi: https://doi.org/10.21134/zt4eht31.

[61] Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, Suplemento, 26 de mayo de 2021, art. 4.

[62] "La venganza pornográfica (revenge porn), también conocida como 'no consentida' como: la distribución en línea de fotografías o vídeos sexualmente explícitos sin el consentimiento de la persona que aparece en las imágenes". María de los Ángeles Casabo Ortíz, "Víctimas menores de edad por revenge

consentimiento y daño que causan en las víctimas. Sin embargo, la diferencia recae en que el contenido sintético, no requiere la participación de las personas involucradas en el acto sexual, dado que el agresor recopila una o más imágenes, videos originales u obras auténticas,[63] para generar contenido falso mediante GANs.

La generación de contenido malicioso ha aumentado las investigaciones revelan "Un aumento del 550 por ciento en los videos *deepfake* en línea entre 2019 y 2023, el 98 por ciento de los cuales se consideran "pornografía deepfake" y el 99 por ciento de los cuales están dirigidos a mujeres".[64] En el año 2024, aumentaron un 245%, y se espera que en 2025 supere el 200% adicional, consolidando un ecosistema criminal en expansión.[65] Este tipo de violencia no es ajena a la realidad basada en una estructura que ha generado discriminaciones y vulneraciones sistemáticas a los derechos fundamentales.

En Ecuador, los fraudes con *deepfakes* incluyen suplantación de identidad y manipulación audiovisual y aumentaron un 411% en 2024,[66] estudios recientes revelan que los incidentes incrementaron un 200 %, durante el último año.[67] La cifra es alarmante, así mismo la revista Information Technology, en febrero de 2025 manifiestó que hubo un aumento del contenido pornográfico en un 96%,[68] cuyos videos e imágenes representan figuras femeninas en escenas intimas, constituyendo un riesgo grave para la privacidad, la seguridad emocional y la imagen pública de las víctimas.

La decisión de democratizar la tecnológica *deepfake*, sin una adecuada supervisión plantea preocupación. En el contexto actual, se ha evidenciado una proliferación de este contenido digital, la ausencia de normativa puede ser aprovechada para difundir *deepfakes* pornográficos, con el fin de causar daño. Así, aunque, "[E]sta conducta, no se encuentra tipificada como delito en el código penal, se argumenta que

---

porn: protección jurídica ante los riesgos del "internet inseguro", *Revista Electrónica de Ciencias Criminológicas* 6, nº 7 (2022): 23-25, https://hdl.handle.net/10550/93007.

[63] Walter Benjamín, *La obra de arte en la época de su reproductibilidad técnica* (Buenos Aires: Taurus, 1989), 10-5.

[64] "Research has revealed a 550 per cent increase in deepfake videos online between 2019 and 2023, 98 per cent of which are considered "deepfake pornography" and 99 per cent of which target women". Stephanie Mikkelson, Emily Springer, y Nora Piay Fernández, *An infographic guide to an infographic guide to TFGBV* (New York: UNFPA, 2025), 11-20.

[65] Nathalia Polo, "IA contra deepfakes al vuelo: el escudo digital de 2025", *WhatsNew*, accedido 16 de septiembre de 2025, párr. 2, https://acortar.link/AhgRmd.

[66] Pamela Proaño, "¿Ciberseguridad en Ecuador? Deepfakes, ransomware y lo que no estás viendo", *Equinoccio Digital*, accedido 12 de junio de 2025, párr. 8, https://equinocciodigital.com/ciberseguridad-ecuador-amenazas-deepfakes-prevencion/.

[67] Sinaluisa Sagñay, Romero Noboa, y Freire, "Deepfakes Pornográficos: Impacto jurídico probatorio y social en el Ecuador", 56.

[68] Ibíd., 45.

constituye una forma actual de violencia de género",[69] las cifras antes mencionadas pueden corroborar esta afirmación, ya que la mayor población afectada son las mujeres.

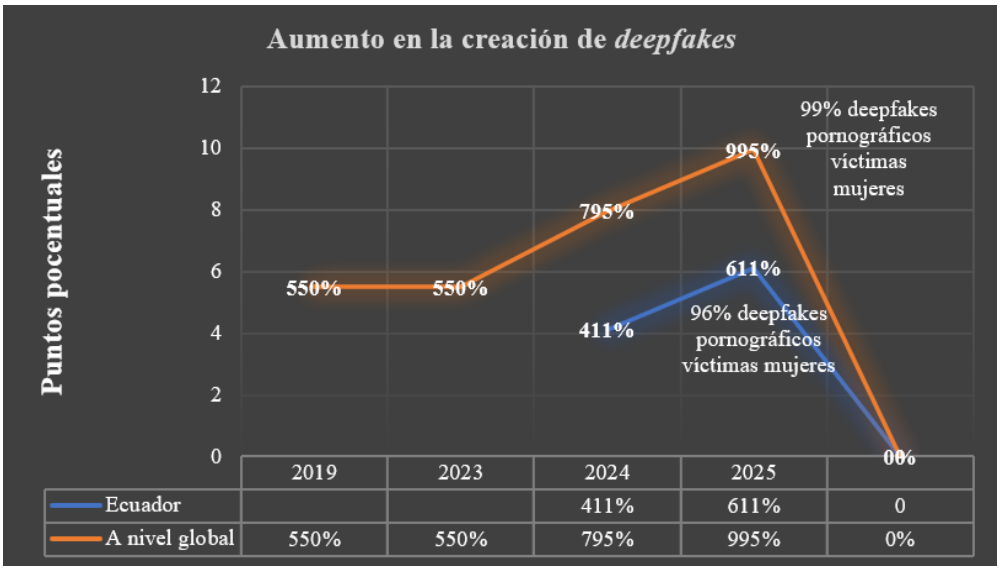


Figura 3. Porcentaje de *deepfakes* pornográficos, Aumento en la creación y difusión de *deepfakes*, 2025
Fuente: Adaptado de Sinaluisa et al.[70] y Mikkelson et.al[71]

En la gráfica se ilustra el aumento en la difusión de *deepfakes* pornográficos, tanto a nivel global como en Ecuador, en base a las cifras previamente analizadas. El mal uso de las creaciones tecnológicas no ha revertido las dinámicas estructurales; al contrario, han contribuido a su intensificación. Un informe de Naciones Unidas en 2015 señala que "Un 73% de mujeres ya había sufrido algún tipo de violencia online".[72] Evidenciando que cuando la tecnología aún no alcanzaba el desarrollo actual, ya existía un elevado porcentaje de violencia digital dirigida hacía las mujeres.

Las dinámicas de agresión se intensificaron con la mala utilización de la IA y los modelos generativos, generando contenido que perjudica a las personas y amplifica el daño. Resulta importante aclarar que si bien, "El 99% de las víctimas de deepfakes pornográficos son mujeres, los hombres también son afectados".[73] Esto implica que cualquier persona puede ser víctima de la creación de *deepfakes* pornográficos,

[69] María Luisa Pereira Hernández y Virginia Mirella Zatarain Avendaño, "Pornografía deepfake en la era de la IA: nuevos desafíos para la educación de género, humanística y tecnológica", *RECIE. Revista Electrónica Científica de Investigación Educativa* 8, nº 10 (2024): 3, doi:10.33010/recie. v8i0.2337.

[70] Sinaluisa Sagñay, Romero Noboa, y Freire, "Deepfakes Pornográficos", 12-20.

[71] Mikkelson, Springer, y Piay Fernández, *An infographic guide to an infographic guide to TFGBV*, 21-5.

[72] Elisa Simón Soler, "Retos jurídicos derivados de la Inteligencia Artificial Generativa", *InDret* 2, nº 12 (2023): 6, doi:10.31009/indret. 2023.i2.11.

[73] Blanca Bayo Pérez, "Los deepfakes pornográficos aumentan un 464% con la mujer como víctima principal", *Verifica RTVE*, accedido 1 de octubre de 2025, párr. 1, https://acortar.link/2SLFi8.

indistintamente de su género, la afectación masculina de esta tecnología también existe y debe ser visibilizada, especialmente en entornos de burla o daño reputacional.

Sin embargo, la mayor afectación según muestran las cifras porcentuales se ha visto en la población femenina, estos datos no pueden ser ignorados ya que evidencian una modalidad específica de violencia digital con sesgo de género, por tanto, reconocer esta dimensión no implica invisibilizar otras formas de afectación. La reiteración de patrones de exposición, vulneración y estigmatización en entornos digitales revela una falla estructural en los mecanismos de protección y también una reproducción de las desigualdades históricas en los entornos tecnológicos.

2.1. Metodología empleada y primer caso de *deepfakes* pornográficos

El presente acápite aborda dos historias de vida de víctimas de *deepfakes* pornográficos, con el propósito de visibilizar la profunda afectación de la violencia digital hacía los derechos fundamentales, en entornos sociales, familiares y educativos. Previo a iniciar, con el estudio de casos se debe señalar que la presente investigación aborda un fenómeno tecnológico emergente que por su naturaleza es transversal, por ello la metodología utilizada para la elección de estudio de casos fue la triangulación cualitativa, que según la autora Angela Torres se puede definir como:

> […] el empleo de diferentes estrategias para estudiar el mismo problema, lo cual se expresa mediante la aplicación de diferentes técnicas para obtener los datos, la presencia de diferentes investigadores para un mismo análisis, la consideración de diversas fuentes de información o la asunción de diferentes teorías para explicar un mismo fenómeno; todo ello con la intención de reforzar el conocimiento y poder verificar la validez de los resultados.[74]

La triangulación cualitativa, empleada en esta investigación es importante porque permite abordar el problema desde tres enfoques, que se integraron a través de las teorías metodológicas como el *process tracing*, el muestreo teórico y el muestreo intencional, a partir del estudio de dos casos concretos, desde el recorrido del daño, la teoría previa y categorías previamente determinadas. Además, las entrevistas siguieron el esquema de la técnica de historia de vida, lo que facilitó comprender ambos casos desde la mirada de las víctimas.

[74] Angela Esther Torres Ruiz, "El transitar en la investigación cualitativa: un acercamiento a la triangulación", *Revista Scientific* 6, nº 20 (2021): 11, doi: 10.29394/Scientific.issn.2542-2987.2021.6.20.15.275-295.

A continuación, se presenta una tabla que resume la triangulación cualitativa:

Tabla 2
Triangulación metodológica para el estudio de casos

Metodología / técnica	Definición	Uso en la presente investigación
Process Tracing	Método que reconstruye paso a paso cómo ocurre un fenómeno.	Sirvió para seguir el camino del daño de los *deepfakes* pornográficos, desde su creación, difusión, hasta la respuesta institucional.
Muestreo Teórico	Selección de casos que ayudan a desarrollar o contrastar una teoría emergente.	Los casos de Simón y Sofía (seudónimos), permiten entender distintas formas de afectación según el género y la edad, además de construir categorías como la violencia digital en el ámbito educativo.
Muestreo Intencional	Selección de casos según criterios definidos previamente	Los casos fueron elegidos mediante criterios como un antecedente de caso abordado por el autor Byron Andino, criterios de género, edad, rol académico, y accesibilidad testimonial en el contexto ecuatoriano.
Historia de vida	Técnica que reconstruye la trayectoria personal de alguien, no solo un hecho puntual.	Esta técnica sirvió para comprender el daño en la vida de Simón, Sofía y María (madre de Sofía), cuidando su dignidad y contexto emocional.

Fuente: George Alexander & Andrew Bennett,[75] Barney Glaser & Anselm Strauss,[76] Michael Patton[77] y Oscar Jara[78]
Elaboración propia

En Ecuador, el uso nocivo de la IA tuvo inició en el ámbito escolar en el año 2023, según reportes "Dos estudiantes hombres crearon con sus dispositivos y aplicaciones de IA más de 700 videos y fotos pornográficas de al menos 24 estudiantes mujeres colegiales (al momento no se conoce el número certero de víctimas)".[79] Las víctimas eran adolescentes que fueron seleccionadas previamente por sus agresores, quienes resultaron

[75] George Alexander y Andrew Bennet, *Case Studies and Theory Development in the Social Sciences* (Cambridge: MIT Press, 2005), 205–32.

[76] Barney Glaser y Anselm Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research* (Chicago: Aldine Publishing Company, 1967), 45–61.

[77] Michael Patton, *Qualitative Research & Evaluation Methods: Integrating Theory and Practice* (California: SAGE Publications, 2014), 230–46.

[78] Oscar Jara Holliday, *La sistematización de experiencias: práctica y teoría para otros mundos posibles* (Bogotá: Centro Internacional de Educación y Desarrollo Humano, 2018), 93–100.

[79] Byron Andino Vélez, "Deepfake, cinismo y diversión en la crueldad: Un caso de colegiales y pornografía en Ecuador", *Uru: Revista de Comunicación y Cultura* 11, nº 2 (2025): 16, doi:10.32719/26312514.2025.11.2.

ser sus propios compañeros de clase. Este suceso, devela la actitud dañina, de los dos adolescentes que generaron contenido pornográfico no consentido.

Por otro lado, se evidencia la falta de control en el acceso de estas herramientas digitales y la ausencia de acción por parte de los padres y autoridades ante la gravedad de la situación, que posteriormente generó la impunidad del hecho. Sofía, quien actualmente tiene 15 años, vive junto a su madre en el Barrio de los Chillos, un día aparentemente normal, recibió una noticia que impacto profundamente su vida, al enterarse que su imagen estaba siendo difundida en redes sociales en videos de contenido pornográfico.

Sofía (seudónimo), recordando lo vivido con tristeza, relata:

> Yo no sabía que se podía hacer algo así…usaron inteligencia artificial para crear un vídeo sexual con mi cara. El vídeo me lo mostró una amiga y sí era mi cara, pero no era yo, […] ya estaba en Tik Tok. Le avisé al tutor, dijo que me iba a ayudar, pero al final no hizo nada. Yo me puse a llorar, lloré mucho, no sabía qué hacer. Llegué del colegio y me encerré en mi cuarto, no quería salir, ni hablar con nadie. Sentía mucha vergüenza de que mis amigos y mi familia vieran el vídeo y pensarán que era yo.[80]

En el relato se evidencia la profunda tristeza de Sofía al tener que encarar esta situación, siendo aún una adolescente y sin apoyo. El impacto que tuvo el hecho en su vida fue profundo especialmente en el plano emocional. Ella menciona que acudió al tutor de curso, esperando recibir ayuda, pero este docente lejos de activar la ruta institucional establecida en la normativa vigente y en el Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación,[81] decide guardar silencio y hacer caso omiso al pedido de auxilio de la estudiante.

Está omisión es el inicio de una serie de vulneraciones a los derechos por parte de la institución educativa, docentes y padres de familia. En la situación específica, el tutor tenía la obligación de comunicar el caso al rector y al Departamento de Consejería Estudiantil (DECE), al no hacerlo impidió la contención emocional de las víctimas, permitiendo una escalada de violencia, obstaculizando el acceso a la justicia y la reparación integral. Ante la falta de acción en su colegio, Sofía al llegar a su casa le comentó a su madre lo sucedido.

María (seudónimo), madre de Sofía al recordar este hecho, relata lo siguiente: “Cuando me enteré de que estaban circulando fotos de contenido sexual de las guaguas, denuncié ante las autoridades del colegio. Esperaba que las protegieran, pero no hicieron

[80] Sofía León, entrevistada por la autora, 14 de julio de 2025. Para leer la entrevista completa, ver Anexo 1.

[81] Ecuador, *Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación*, Registro Oficial 401, Suplemento, 21 de octubre de 2023, art. 3.

nada…incluso parecía que la institución trataba de encubrir el hecho, nos silenciaban el micrófono y nos decían el grupito de padres que tiene ese problema".[82] Se trataba de menores de edad que habían sido expuestas mediante una red social de amplia difusión y las autoridades no hacían nada para detener esta vulneración.

Al aislar a las víctimas y además llamarlos el grupito con ese problema, se evidencia una situación de estigmatización y encubrimiento por parte de la entidad educativa. La Corte Constitucional, en su sentencia N.º 1497-20-JP/21,[83] ha mencionado que impedir el acceso a mecanismos de denuncia afecta el desarrollo de niñas, niños y adolescentes. Además, "La declaración de la vulneración de derechos genera la obligación de reparar el daño causado".[84] Por tanto, el establecimiento no sólo silenció los reclamos de las víctimas, sino que incumplió su deber de reparación integral.

Según, la Norma Técnica del Servicio de Atención y Protección Emergentes del MIES[85] y el Protocolo para Atención a Víctimas de Violencia de Género e Intrafamiliar,[86] se trata de un caso de violencia digital que afectó derechos como la imagen, intimidad e integridad personal, social y simbólica de las estudiantes. Además de derivar el hecho a Junta Cantonal de Protección de Derechos, de acuerdo al Código de la Niñez y Adolescencia.[87] El DECE, debió brindar asistencia, apoyo psicológico a las víctimas y emitir un informe detallado de la situación.

Finalmente, si existía indicios de responsabilidad penal como la difusión de contenido sexual no consensuado, la institución debió notificar a Fiscalía, activando los canales penales correspondientes y actuando conforme al principio de interés superior del niño, niña y adolescente establecido en Constitución,[88] precautelando los derechos de las

---

[82] María León, entrevistada por la autora, 15 de julio de 2025. Para leer la entrevista completa, ver Anexo 2.

[83] Ecuador Corte Constitucional, "Sentencia", *Juicio n.°: 1497-20-JP/21*, 21 de diciembre de 2021, 10.

[84] Ibíd., 17.

[85] Ecuador, *Norma Técnica del Servicio de Atención y Protección Emergentes del MIES*, Registro Oficial 694, Suplemento, 29 de noviembre de 2024, art. 5.

[86] Ecuador, *Protocolo para la atención de llamadas de emergencia relacionadas con violencia de género e intrafamiliar recibidas por el ECU-911*, Registro Oficial 411, Suplemento, 05 de octubre de 2023, art. 6.

[87] "[…] Deber jurídico de denunciar. - Toda persona, incluidas las autoridades judiciales y administrativas, que por cualquier medio tenga conocimiento de la violación de un derecho del niño, niña o adolescente, está obligada a denunciarla ante la autoridad competente, en un plazo máximo de cuarenta y ocho horas". Ecuador, *Código de la Niñez y Adolescencia*, Registro Oficial 737, Suplemento, 03 de enero de 2003, art. 17.

[88] "[…] El Estado, la sociedad y la familia promoverán de forma prioritaria el desarrollo integral de las niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos; se atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas". Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, Suplemento, 20 de octubre de 2008, art. 44.

menores afectadas. Aunque la Fiscalía sí inició una investigación formal, esta no logró avanzar ni derivó en un proceso judicial penal, precisamente porque el hecho no se encontraba tipificado en el ordenamiento jurídico vigente.

Respecto a los días posteriores al hecho, Sofía menciona:

> Yo me sentía cada vez más triste. En el cole hubo compañeros que nos apoyaron, pero también full gente que nos miraba feo, que hablaba mal de nosotras… decían que éramos fáciles, que buscábamos problemas, como si todo hubiera sido culpa nuestra. Y pasaban los días y nadie decía nada. No hubo consecuencias, ni una charla, ni disculpas, nada. Fue como si no importara lo que nos hicieron. Y eso… eso es lo que más dolió. Que todo quedara así, como si nunca hubiera pasado.[89]

El art. 66 num. 3, de la CRE[90] reconoce el derecho de la integridad física, psíquica y moral de las personas; mismo que fue vulnerado cuando la víctima no recibió atención psicológica adecuada. Además, el hecho que la llamaran problemática o fácil, refleja una sociedad que culpabiliza a las víctimas y reproduce estigmas. Además, se transgrede el derecho a la protección contra todo tipo de violencia, incluida la digital estipulada en los arts. 35 y 46 de la misma norma suprema,[91] que garantiza la protección y no revictimización.

La afirmación de Sofia, respecto a la falta acción por parte de la institución, revela el profundo dolor ante la indiferencia de las autoridades, docentes y sus compañeros, evidenciando la impotencia frente a una sociedad indolente, que posiblemente por tratarse de un hecho inédito y que involucra nuevas herramientas tecnológicas no supo cómo reaccionar. Pues si bien, las imágenes se originaron en un entorno virtual, los daños fueron reales y Sofia al igual que sus compañeras, lo vivió en espacios cotidianos, siendo discriminadas y silenciadas.

Ante estos hechos María, menciona la forma en que su familia abordo esta situación:

> Mi hija y yo pasamos noches enteras en vela, sin poder dormir. Ella lloraba, y nosotros estábamos angustiados, sin saber qué hacer, sintiéndonos solos frente a algo que nos sobrepasaba. Pero lo que más me marco fue la indiferencia de la sociedad, en especial de la institución educativa y de los otros padres de familia. Cerraron las puertas frente a un problema grave, y no hicieron nada por ayudar. […] Acudimos al DECE, ellos tenían los teléfonos celulares de los chicos, tuvieron la evidencia todo el tiempo y realmente no hicieron nada […][92]

---

[89] Sofía León, entrevistada por la autora, 3.

[90] "[…]Se reconoce y garantizará a las personas: [...] 3. El derecho a la integridad personal, que incluye: a] La integridad física, psíquica, moral y sexual". Ecuador, *Constitución de la República del Ecuador*, art. 66.

[91] Ibíd., 16.

[92] María León, entrevistada por la autora, Anexo 2.

La violencia digital impactó a la familia, revelando el abandono emocional y social, al que muchas víctimas se ven expuestas. María, menciona que fue triste ver a su hija sin tener el apoyo necesario por parte de quien debería brindarlo. Además, dice que la institución tenía los teléfonos de los chicos y no hizo nada, configurándose la primera vulneración al derecho de la dignidad, la justicia y la reparación integral consagrados en los arts. 11 y 75 de la CRE.[93] Finalmente, la institución educativa decide ignorar por completo a las víctimas.

En esa situación, María relata que:

> Después de casi un mes, logramos contactar con una fundación. Una abogada nos escuchó, creyó en nosotras y ayudó a visibilizar el caso. No queríamos exponer a nuestras hijas, pero era la única forma de ser escuchadas. Con la presión mediática, los chicos fueron retirados de la institución. Al día siguiente, tuvimos una sesión virtual con la Fiscalía. Fue corta, dijeron que habría investigación, pero que sería lenta, debido a que no había muchos registros ni una normativa clara, y que no se podía hacer mucho.[94]

María debía precautelar la intimidad de su hija, pero también comunicar la situación ocurrida para recibir ayuda, la falta de apoyo obligó a esta familia a exponerse públicamente ante los medios, corriendo el riesgo de ser revictimizadas con el fin de recibir ayuda. El accionar de la abogada de denunciar públicamente lo sucedido constituyó una ayuda, visibilizando la violencia digital a la cual fueron sometidas las víctimas. El art. 66 núm. 20,[95] de la Constitución garantiza la intimidad, como un derecho primordial del individuo en la esfera personal, familiar y social.

Asimismo, el art. 6 del Código de la Niñez y Adolescencia[96] establece el principio de igualdad, asegurando la protección sin distinción alguna, incluida la situación de vulnerabilidad de las estudiantes. El retiro de los dos adolescentes evidencia un problema en el accionar de los padres, encubriendo el hecho de violencia ofreciendo una compensación económica, a cambio de evadir la responsabilidad. Esta acción no sólo trata de minimizar el daño, sino que también refuerza una cultura de impunidad,[97] que prevalece en sociedades injustas y marcadas por la corrupción.

---

[93] Ecuador, *Constitución de la República del Ecuador*, arts. 11-75.
[94] María León, entrevistada por la autora, anexo 2.
[95] Ecuador, *Constitución de la República del Ecuador*, art. 66.
[96] Ibíd., art. 6.
[97] "Nosotros consideramos que la expectativa de impunidad relacionada con los actos de corrupción funciona como un contexto que incentiva su comisión, que mantiene la comisión de actos corruptos a lo largo del tiempo, y que todo ello impacta en la disminución del ejercicio de los DH. En este marco, corrupción e impunidad se convierten en patrones estructurales de las violaciones a los DH". Daniel Vázquez y Horacio Ortiz, "Impunidad, corrupción y derechos humanos", *Perfiles Latinoamericanos* 29, nº 57 (2021): 4, doi:10.18504/pl2957-007-2021.

La Fiscalía mediante Zoom había afirmado que no pueden hacer mucho, dejando al descubierto la falta de diligencia judicial y una vulneración directa a las garantías procesales mínimas que deben regir en cualquier proceso legal. Esta omisión compromete el derecho de acceso a la justicia consagrado en el art. 75 de la Constitución de la Republica del Ecuador,[98] el principio de tutela judicial efectiva y la debida diligencia, tipificados en el art. 2 del COIP,[99] aumentando aún más la situación de impunidad y falta de acción ante lo sucedido.

Finalmente, Sofia menciona lo siguiente:

> Yo ya no quería ver a mi mamá tan triste, así que ella decidió sacarme del colegio. Al principio fue duro, pero después me enteré que las otras chicas siguieron con sus vidas, estaban más tranquilas y ya nadie hablaba mucho del tema. Lo raro, es que ahora se ve normal que tu cara aparezca en el cuerpo de otra persona haciendo bailando o riéndose, como si fuera un meme. Pero cuando te pasa algo así, lo ves diferente. Es como que todos creen que porque es virtual no te afecta, pero sí afecta. Por suerte yo logré salir de todo ese lío, pero fue muy difícil.[100]

Sofía es consciente que la violencia digital continúa normalizándose, bajo la apariencia de humor. La manipulación del rostro de una persona en un cuerpo ajeno realizando actos denigrantes, no se encuentra tipificada en la norma penal, sin embargo, constituye una afectación directa a la dignidad e invita a cuestionarse la forma que se comparte y manipula la información en la sociedad liquida planteada por Bauman.[101] Es necesario pensar en una realidad más consciente de la materialidad del sufrimiento que puede generar el contenido digital dañino y el deber de cuidado de la información.

2.2. Segundo caso: docente víctima de *deepfakes* pornográficos

El segundo caso corresponde a un hombre que, además de ser esposo y padre de familia, se desempeña como docente en una institución de educación superior. Siendo una víctima de violencia digital a través de la difusión de *deepfakes* de contenido pornográfico no consentido, lo que generó una grave afectación a su imagen pública y tuvo repercusiones directas en su entorno laboral y familiar.

---

[98] "Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley". Ecuador, *Constitución de la República del Ecuador*, art. 75.

[99] "Principios generales. - [...] En particular se aplicarán los principios de tutela judicial efectiva y debida diligencia a fin de garantizar la reparación integral para las víctimas y la prevención de la reincidencia y de la impunidad". Ibíd., art. 2.

[100] Sofía León, entrevistada por la autora, 2.

[101] Zygmunt Bauman, *Modernidad Líquida*, (Madrid: Fondo de Cultura Económica de España, 2000), 7-10.

Así comienza la historia de Simón (seudónimo), quien relata lo siguiente:

> Al asumir la dirección de la carrera de pregrado en la Universidad, fui convocado por el rector a una reunión urgente con autoridades académicas. Allí me mostraron siete imágenes, algunas tomadas de sesiones por zoom durante la pandemia, donde aparezco vestido formalmente, impartiendo clases. Sin embargo, otras fotografías mostraban una toma desde debajo del escritorio en la que se me veía con los genitales expuestos. Estas imágenes, evidentemente alteradas mediante técnicas de *deepfake*, estaban acompañadas por un mensaje que decía: "Miren cómo el doctor trata con una niña de 12 años".[102]

Simón fue víctima de violencia digital mediante la exposición de imágenes que comprometían su intimidad e integridad construyeron una narrativa falsa y causaron una profunda afectación. En ese sentido, se vulneró el derecho a la honra y reputación dispuesto en el art. 66 núm. 18 de la CRE.[103] La manipulación de imágenes y el mensaje que lo acompaña, vinculan al docente a un posible delito de pornografía infantil[104] tipificado en el art. 103 del Código Orgánico Integral Penal.

La Corte Interamericana de Derechos Humanos[105] (CIDH), establece que "El derecho de la víctima o de sus familiares a obtener de los órganos competentes […] el esclarecimiento de los hechos violatorios y las responsabilidades correspondientes, a través de la investigación y el juzgamiento que previenen de los artículos 8 y 25, lo cual constituye una forma de reparación".[106] Por tanto, al aceptar las imágenes que simulaban ser reales, las autoridades acusaron a Simón de una historia ajena, esta imposición afectó de manera directa su credibilidad en su entorno laboral.

Al continuar su relato, Simón comenta que:

---

[102] Simón Rivas, entrevistado por la autora, 15 de julio de 2025. Para leer la entrevista completa, ver Anexo 3.

[103] "Se reconoce y garantizará a las personas: [...] 18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona". Ecuador, *Constitución de la República del Ecuador*, art.66.

[104] "Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años". Ecuador, *Código Orgánico Integral Penal COIP*, Registro Oficial 180, Suplemento, 10 de agosto de 2014, art.103.

[105] Se hace referencia a los derechos humanos debido a que el marco internacional ofrece bases jurídicas más sólidas que la ética para establecer controles y límites al poder en la era digital. Define conductas aceptables, ya acordadas por los Estados, y cuenta con instrumentos como la Declaración Universal, convenios, tratados, tribunales y comisiones que permiten exigir responsabilidades tanto a Estados como a empresas. Véase en ONU, "Derechos humanos en la era digital", *Organización de Naciones Unidas (ONU)*, accedido 7 de agosto de 2025, párr. 15, https://www.ohchr.org/es/2019/10/human-rights-digital-age.

[106] Corte CIDH, "Sentencia de 24 de noviembre de 2011 (Excepciones Preliminares, Fondo, Reparaciones y Costas)", *Caso Familia Barrios vs. Venezuela*, 24 de noviembre de 2011, párr. 291, https://corteidh.or.cr/docs/casos/articulos/seriec_237_esp.pdf

> Comenzaron a circular imágenes explícitas que parecían mostrarme con el órgano genital expuesto. […] Las imágenes eran increíbles, a primera vista no es que cuestionabas. Esas fotos que parecían sacadas de una película para adultos. me sorprendieron, ellos insistían a ver si no se me habían filtrado esas fotografías, a lo que yo también me molesté, porque les dije yo no me había tomado este tipo de fotos. […] el ángulo era imposible, y parecía como si zoom transmitiera desde varios puntos, incluso debajo del escritorio, eso era absurdo. Fue el gerente de la universidad quien, al verlas, sugirió por primera vez que podrían haber sido generadas con inteligencia artificial.[107]

Las imágenes generadas por IA no sólo vulneraron la intimidad del docente; sino que lograron desprestigiarlo públicamente. El realismo visual de las imágenes, aunque él mismo sabía que no eran auténticas, intensificó el impacto del daño. Simón dice que acuerdo al ángulo era imposible que fueran verdaderas pero que tampoco podía probar que eran simuladas. Al respecto el art. 12 de la Declaración Universal de los Derechos Humanos (DUDH),[108] reconoce la intimidad, la honra y reputación como derechos del ser humano y exige su protección frente a cualquier forma de agresión.

Respecto al creador de estas imágenes, Simón sostiene que "[L]as enviaba en una cuenta de nombre Burkina Facio, la cuenta aparentemente no era de Ecuador estaba bastante extraño. Las autoridades, estaban preocupados por la insistencia también era bajo amenaza de que se les pague para que ya no sigan enviando esas fotos".[109] En este punto se observa que la violencia digital se dirige al chantaje económico, la amenaza de difundir las imágenes y la ambigua preocupación de las autoridades.

El daño no sólo es a la intimidad también existe afectación patrimonial que puede enfrentar la víctima y el desprestigio de su imagen profesional. La difusión de las imágenes a través de una cuenta falsa imposibilita la identificación del responsable y es un obstáculo para la atribución de la responsabilidad penal.[110] Siendo casi imposible determinar la autoría, en este contexto esta acción se puede relacionar al delito de extorsión tipificado en el art. 185 del COIP, que sanciona las amenazas que buscan obtener un beneficio económico en perjuicio del patrimonio de la persona.

No obstante, aunque la normativa penal prevé este hecho, no regula los casos en que las imágenes pudiesen ser generadas mediante IA generativa, como ocurre con los *deepfakes* pornográficos. Esta omisión evidencia un vacío jurídico preocupante al

---

[107] Simón Rivas, entrevistado por la autora, Anexo 3.

[108] ONU Asamblea General, *La Declaración Universal de los Derechos Humanos*, 10 de diciembre de 1948, núm. 12, A/RES/217/ 3.

[109] Simón Rivas, entrevistado por la autora, Anexo 3.

[110] "El delito informático es más difícil de investigar que el delito tradicional porque es novedoso, escapa a los cánones tradicionales, los cuerpos policiales y tribunalicios no están preparados para investigar y detectar estas técnicas novedosas y el propio delito no suele dejar rastros". Pablo Palazzi, *Delitos Informáticos* (Buenos Aires: AD-HOC Sociedad de Responsabilidad Limitada, 2000), 70-82.

momento de enfrentar, las nuevas formas de violencia digital. Continuando con su relato, Simón comparte las acciones que emprendió tras lo sucedido:

> Me indicaron que tomara ciertas precauciones, pero nunca recibí las comunicaciones que habían enviado a la universidad; solo llegó un mensaje extraño que bloqueé, aunque me quedó la sensación de que alguien cercano conocía el asunto. Empecé a desconfiar de las notificaciones institucionales, y aunque no parezca, ese episodio terminó afectando mi carrera: tenía posibilidades reales de ser decano, pero todo comenzó a jugar en mi contra. La situación se agravó por el vínculo conservador de la universidad con el Opus Dei, […] Ese mismo día, el rector me pidió que llamara a mi esposa para hablar del tema; fue incómodo, pero hice la llamada.[111]

Se cuestiona la decisión de las autoridades al solicitar que se involucre a su esposa sin una justificación y siendo una vulneración al derecho de intimidad personal. En el transcurso de los hechos no se observa que se haya garantizado el derecho a la defensa ante una situación que afectó en gran medida su prestigio y carrera en la institución educativa. La vinculación de la institución al Opus Dei sugiere posibles sesgos que podrían influir en la decisión de las autoridades, quienes deberían emitir sus decisiones de manera objetiva e imparcial, según lo manifestado en la Constitución.

Finalmente, Simón menciona lo siguiente:

> Por todo lo que había hecho profesionalmente, tengo cierto nivel de reconocimiento. Lo que ocurrió parecía claramente una campaña de desprestigio. Tras presentar la denuncia, un policía inició la investigación y verificó mi posicionamiento en redes sociales, especialmente en Facebook. Detectó que el número involucrado provenía de una plataforma digital, probablemente vinculada a la cárcel de Latacunga. Me explicó que alguien buscaba dañar mi imagen, además de tener un claro interés económico. Me recomendó transparentar el asunto públicamente, con un comentario o aviso general en Facebook. Han pasado tres años, y desde entonces no se ha hecho nada más.[112]

Simón relata la forma que logró denunciar el hecho y hacerlo público con el fin de evitar repercusiones especialmente en su vida laboral, ya que su vida personal no se vio tan afectada, según el mismo menciona. El número desde el que se enviaba las imágenes nunca llegaron al teléfono de Simón Rivas, el policía detecto que provenían de una cárcel de Latacunga, configurando un posible delito de estafa con la clara intención de desprestigio que terminó provocando la renuncia del docente, además de afectar su posible ascenso en esta institución de educación superior.

[111] Simón Rivas, entrevistado por la autora, anexo 3.
[112] Ibíd., 4.

En base a los dos casos expuestos en este estudio, se presenta a continuación un cuadro comparativo, que sintetiza los posibles impactos en la vida de ambas personas, considerando sus diferentes dimensiones.

Tabla 3
Cuadro comparativo del impacto de *deepfakes* pornográficos

Dimensión	Primer caso: Sofía León (seudónimo)	Segundo Caso: Simón Rivas (seudónimo)
Íntima	Vergüenza corporal Miedo a ser confundida con el contenido falso	Exposición genital simulada. La nitidez impide distinguir la falsedad visual
Familiar	Temor al juicio de sus familiares Impacto emocional en la familia (madre)	Obligación por parte de la institución de comunicar el hecho a su esposa Incomodidad familiar
Laboral y Escolar	Falta de activación del protocolo educativo. Ausencia de contención emocional institucional.	Acusación institucional basada en imágenes falsas Pérdida de oportunidades profesionales.
Social	Exposición pública en TikTok	Circulación de imágenes explícitas a través de mensajes WhatsApp
Legal	Omisión del deber de denuncia por parte del tutor Vulneración de la dignidad y derechos personales como la intimidad y la imagen	Vulneración del derecho a la inocencia, por asumir la culpa Posible vinculación con delitos graves (pornografía infantil, extorsión)
Emocional	Llanto constante aislamiento Desesperación Ausencia de apoyo	Frustración ante la falta de protección Daño a la trayectoria profesional

Fuente: Testimonios de Sofía León, María León y Simón Rivas (seudónimos)
Elaboración propia

3. La posverdad: impacto de los *deepfakes* pornográficos en la confianza social

Los *deepfakes* pornográficos han provocado una afectación significativa en la confianza social al permitir engaños elaborados a través de "[R]elatos y representaciones falsas con escaso control por parte de autoridades, instituciones, ciudadanos y la insuficiente regulación por las propias plataformas".[113] Inducen a aceptar contenido que se presenta como genuino, provocando una desconfianza generalizada hacia el entorno digital. En el contexto actual de posverdad, se han integrado como la nueva normalidad, difuminando los límites entre la realidad y lo creado artificialmente.

[113] Lucia Ballesteros Aguayo y Francisco Javier Ruiz Del Olmo, "Vídeos Falsos y Desinformación Ante la IA: el Deepfake como Vehículo de la Posverdad", *Revista de Ciencias de la Comunicación e Información* 29, nº 1 (2024): 2, doi:10.35742/rcci.2024.29. e294.

Figura 4. *Deepfake* que muestra al papa Francisco como un modelo de Balenciaga, mientras la imagen de la derecha se encuentra Donald Trump siendo detenido, 2023
Fuente: Imagen de elDiario.es[114]

La pérdida de confianza impacta en las plataformas digitales, tales como Meta y Tik Tok, mediante las mismas se comparten una variedad de publicaciones falsas. En el contexto digital, la posverdad se construye como "Una estrategia discursiva intencionada, que persigue establecer una idea como verdadera a partir de una manipulación de información, hechos, actos, emociones, actores y escenarios mediáticos".[115] Se basa en el engaño y en la viralización de la información, nunca antes se había cuestionado la capacidad de los sentidos para discernir la realidad.

El contenido falso y dañino, distorsiona la percepción de la realidad y representa un riesgo para la sociedad. Kevin Mitnick, ex hacker y una destacada figura en ciberseguridad, en su libro *The art of invisibility*, manifiesta que "La ingeniería social es una técnica de hacking que utiliza la manipulación, el engaño y la influencia para lograr que una persona cumpla con una solicitud. A menudo, se engaña a las personas para que proporcionen información confidencial".[116] En la difusión de contenido falso, la ingeniería social es utilizada para la manipulación psicológica de los espectadores.

Resulta interesante comprender que esta técnica, no sólo se basa en la manipulación de los sistemas tecnológicos, sino que también se centra en las emociones personales como la confianza, la validación, el temor o la vergüenza de ser expuesto. Mientras el contenido de carácter explícito aún no ha sido difundido, el agresor actúa a través de amenazas exigiendo una compensación económica a cambio de no hacerlo,

[114] elDiario.es, "El papa moderno o Trump detenido: llega la realidad paralela de la inteligencia artificial", *El Diario*, accedido 31 de marzo de 2023, https://n9.cl/wx80e.

[115] Bañuelos Capistrán, "Deepfake: la imagen en tiempos de la posverdad", 3.

[116] "Social engineering is a hacking technique that uses manipulation, deception, and influence to get a human target to comply with a request. Often people are tricked into giving up sensitive information". Kevin Mitnick, *The art of invisibility* (New York: Little, Brown and Company, 2017), 36 - 40.

cuando el material ya haya sido difundido, los daños se intensifican afectando a la víctima, pero ese sólo es el primer paso para amenazas más complejas.

Las redes sociales de Meta, como Facebook, Instagram o WhatsApp, han sido el centro de atención por la difusión de contenido pornográfico no consentido; estas plataformas operan a través de algoritmos, entendidos como "Un conjunto ordenado de pasos para resolver un problema determinado".[117] La ingeniería social se apoya de los mismos para recolectar información y clasificar a las personas según su comportamiento en redes sociales. Un ejemplo, de esta técnica social se trata de la demanda impulsada por la Fiscalía de New York en contra de Meta[118] la empresa matriz de Instagram.

La Fiscalía acusó a Instagram de utilizar algoritmos que inciden en la salud mental de adolescentes, generando depresión y baja autoestima. El impacto se vincula al diseño adictivo del algoritmo, basado en el *scroll*[119] y la validación social a través de *likes.*[120] La demanda reveló que la empresa hacía segmentación social por edad de sus usuarios para maximizar la permanencia en línea. En base a la manipulación algorítmica, existe el caso Cambridge Analytic, sobre la explotación de las convicciones de las personas, utilizando ingeniería social para manipular las decisiones a gran escala.

Este caso, se presentó de la siguiente manera:

> En 2018, Cambridge Analytica acaparó titulares después de las revelaciones de que hizo un mal uso de los datos personales de millones de usuarios de Facebook para construir perfiles de votantes psicográficos para influir en las elecciones. La noticia puso las políticas de privacidad de datos de Facebook bajo un nuevo escrutinio y llevó a las investigaciones de EE.UU. y el Reino Unido sobre Cambridge Analytica y su eventual disolución.[121]

---

[117] Alexander Oviedo Fadul, *Diseño estructurado de algoritmos* (Sincelejo: Imprenor, 2004), 14-18.

[118] BBC News Mundo, "Instagram: más de 40 estados en EE.UU. demandan a la red social por supuestos daños en la salud mental de los adolescentes", *BBC News Mundo*, accedido 30 de agosto de 2025, párr. 5, https://www.bbc.com/mundo/articles/cldxr742rk0o.

[119] "El 'scroll' es el acto de deslizar el dedo hacia arriba o hacia abajo en la pantalla de un dispositivo para navegar por contenido digital, como publicaciones en redes sociales, sitios web, o aplicaciones". Maximiliano Fernández, "El milagroso (o perturbador) algoritmo de TikTok: qué hay detrás de la red social más adictiva", *Infobae*, accedido 4 de septiembre de 2025, párr. 2, https://acortar.link/4485Aa.

[120] Dialoguemos, "Nueva York demandó a cinco redes sociales por la crisis de salud mental en niños y jóvenes", *Dialoguemos. La academia en la comunidad*, accedido 30 de agosto de 2025, párr. 5, https://acortar.link/8bw1PY.

[121] "In 2018, Cambridge Analytica captured headlines after revelations that it misused the personal data of millions of Facebook users to build 'psychographic' voter profiles to influence elections. The news put Facebook's data privacy policies under new scrutiny and led to U.S. and U.K. investigations of Cambridge Analytica and its eventual dissolution". Brendan Fischer, "Newly Published Cambridge Analytica Documents Show Unlawful Support for Trump in 2016", *Campaign Legal Center*, accedido 4 de septiembre de 2025, párr. 7, https://campaignlegal.org/update/newly-published-cambridge-analytica-documents-show-unlawful-support-trump-2016.

Se evidencia la falta de regulación en el uso de información, además se cuestiona la perfilación que influye en la decisión de los votantes, llegando a afectar la libertad de voto y vulnerando la información privada de millones de personas. Este caso, tuvo repercusiones en las elecciones presidenciales de EE. UU. y el referéndum del Brexit.[122] El proceso de segmentación regulada por el Reglamento General de Protección de datos de la UE,[123] que trata de clasificar a las personas en grupos, constituye una práctica digital que vulnera los derechos e información personal.

Al igual que la segmentación, en la creación de *deepfakes* pornográficos se recolecta datos de carácter sensible sin su consentimiento como fotos y videos. El experto en identidad digital Edgar Whitley menciona "Los expertos en seguridad llevan tiempo advirtiendo sobre las amenazas que representan los deepfakes tanto a particulares como a organizaciones",[124] constituyendo una preocupación creciente de la seguridad digital, se trata de una amenaza directa a la dignidad que ha creado eventos ficticios confundiendo y debilitando la confianza en fuentes auténticas.

El aumento en su complejidad sobrepasa la habilidad humana para detectarlos, en un estudio reciente "Los resultados son alarmantes: solo el 0,1 % de los participantes pudo distinguir con precisión el contenido real del falso en todos los estímulos, que incluían imágenes y vídeos".[125] Esta cifra revela no solo una vulnerabilidad cognitiva generalizada, sino también una preocupante brecha en la alfabetización digital. Se evidencia que, incluso cuando las personas sospechan de una posible falsificación, en la mayoría de los casos no lo reportan, facilitando la propagación de ataques en línea.

La reputación y la integridad de individuos y colectivos, se ve comprometida a través de estas creaciones digitales que pretenden alterar la realidad. En otra perspectiva, Walter Benjamín en su libro titulado *La obra de arte en la época de su reproductibilidad*

---

[122] "Se descubrió que durante la campaña se difundió información manipulada, eliminada posteriormente pero que afectó la percepción pública". Camilo Molina Bolívar et al., "La Comunicación y su impacto en la vida democrática de América Latina y el Caribe", *Chasqui: Revista Latinoamericana de Comunicación* 19, nº 141 (2019): 27, file:///C:/Users/cango/Downloads/REXTN-Ch146.pdf.

[123] Unión Europa, *Reglamento General de Proteccion de Datos de la Unión Europea*, Diario Oficial de la Unión Europea, 27 de abril de 2016, arts. 4-89.

[124] "Security experts have been warning of the threats posed by deepfakes for individuals and organizations alike for some time. This study shows that organizations can no longer rely on human judgment to spot deepfakes and must look to alternative means of authenticating the users of their systems and services". Wire Bussines, "iProov Study Reveals Deepfake Blindspot: Only 0.1% of People Can Accurately Detect AI-Generated Deepfakes - Silicon Canals", *Silicon Canals*, accedido 7 de julio de 2025, párr. 10, https://siliconcanals.com/iproov-study-reveals-deepfake-blindspot-only-0-1-of-people-can-accurately-detect-ai-generated-deepfakes/.

[125] Andrew Bud, "Menos del 1% de falsificaciones generadas por IA se detectan: iProov - Revista Mas Seguridad", *Revista Mas Seguridad*, accedido 4 de septiembre de 2025, párr. 2, https://acortar.link/Uy3H4D.

técnica menciona, que "La autenticidad se basa en la presencia irrepetible de una obra desde su aparición hasta su divulgación".[126] La verdad se ve afectada a través de los *deepfakes* pornográficos, ya que el contenido que se recrea simula una falsa realidad y puede llegar a vulnerar los derechos esenciales.

A nivel mundial existe algunos ejemplos, que se puede abordar como la difusión de *deepfakes* pornográficos a través de WhatsApp, en el municipio de Badajoz, España.[127] En Corea del Sur, se registró 800 denuncias en un solo año, por la creación y difusión *deepfakes* pornográficos a través de Telegram.[128] En EE. UU., el caso Westfield High School, los estudiantes crearon *deepfakes* sexuales de sus compañeras y los difundieron en Facebook y debido a la presión de las víctimas se aprobó *Take It Down*,[129] una ley para abordar este tipo de vulneraciones digitales.

En el caso de Kate Isaacs una activista británica en contra de la violencia digital, fue víctima de *deepfakes* pornográficos,[130] la magnitud del daño la desbordó emocionalmente. Un análisis sistemático, explica que "[L]os algoritmos pueden propagar aún más el contenido no consensuado, y los procesos para eliminarlo son lentos y poco efectivos".[131] Así se construye la *legitimidad algorítmica*[132], los *likes* y comentarios logran normalizar este tipo de abuso. La confianza social se ve erosionada por sesgos de confirmación, sin existir herramientas en tiempo real para identificar manipulaciones digitales.

---

[126] Benjamín, *La obra de arte y la reproductibilidad técnica*, 8 - 15.

[127] "El Juzgado de Menores de Badajoz en Sentencia de 20 de junio de 2024, dictó sentencia de conformidad en la que se fijaron como hechos probados que los menores imputados utilizaron una aplicación de IA (ClothOff) para manipular imágenes de otras menores, de ese modo, a través de las imágenes reales de los rostros de las chicas obtenidos de sus perfiles de las redes sociales, les superponían imágenes de otros cuerpos femeninos desnudos". Gema Varona et al., *Victimología Didáctica y Aplicada: Análisis de Casos* (Madrid: Laborum Ediciones, 2025), 16-18.

[128] Jean Manckenzie, "La crisis del porno deepfake que afecta a las escuelas coreanas", *BBC News Mundo*, accedido 30 de agosto de 2025, párr. 3, https://www.bbc.com/mundo/articles/c93p53292kyo.

[129] "Take It Down Act es la primera ley federal de Estados Unidos diseñada específicamente para hacer frente a la difusión de imágenes íntimas no consentidas (NCII, por sus siglas en inglés), incluidas las deepfakes generadas por IA". Alonso Martínez, "Take it Down Act, la ley que criminaliza los deepfakes y la 'pornovenganza'", *El País US*, accedido 30 de agosto de 2025, párr. 2, https://acortar.link/uQTMSp.

[130] "Kate sospechaba que la persona que compartió el vídeo podría ser alguien a quien ella incomodó con su campaña, el mismo contenía comentarios ofensivos, inclusive amenazas en contra de su integridad". Sarah McDermott y Jess Davies, "Deepfake: Pusieron mi cara en un video porno", *BBC News Mundo*, accedido 25 de julio de 2025, párr. 5, https://www.bbc.com/mundo/noticias-63354076.

[131] Barba Arteaga, "Deepfakes sexuales: impacto, prevención y perspectivas de género en el entorno digital", 8.

[132] "[I]s a generalized perception or assumption that the actions of an entity are desirable, proper, and appropriate within some socially constructed system of norms, values, beliefs, and definitions. Traducción: es una percepción generalizada o suposición de que las acciones de una entidad son deseables, adecuadas y apropiadas dentro de algún sistema socialmente construido de normas, valores, creencias y definiciones". Woodrow Barfield, *The Cambridge Handbook of the Law of Algorithms* (Cambridge: Cambridge University Press, 2020), 479 -505.

3.1. *Soft law*: ética y educación digital frente a los *deepfakes* pornográficos

Ante la creciente preocupación por la creación y difusión de contenido digital dañino generado a través de IA, es necesario analizar el *soft law*[133] orientado a la ética y la educación digital desde la perspectiva crítica que la ética aplicada en la tecnología no es neutral, si no que refleja los valores de quienes la crean y utilizan. Respecto a la responsabilidad en cuanto a la creación y difusión de contenido pornográfico no consentido, el análisis de este acápite se centra en tres actores clave: las plataformas digitales, los desarrolladores y los usuarios.

Desde una perspectiva social, se aborda la práctica de comportamientos beneficiosos.[134] Esta disciplina deontológica, aplicada a las nuevas tecnologías como la IA, "Se ocupa del cambio tecnológico y su impacto en la vida de los individuos, como de las transformaciones que se producen en la sociedad y en la economía."[135] En respuesta a los nuevos desafíos de la globalización, las grandes potencias han promovido la creación protocolos éticos, reconociendo que el avance tecnológico exige instrumentos de contingencia que orienten su desarrollo y aplicación.

Dichos protocolos, como la Recomendación sobre la ética de IA de la UNESCO de 2021, [136] o la Declaración de Montreal para una IA responsable en 2017 así como los cincos principios para un Código de IA de Reino Unido de 2017,[137] tienen como objetivo asegurar la responsabilidad y transparencia, desde el inicio del desarrollo de estas tecnologías. La adopción de protocolos éticos no solo resulta necesaria, su generalización es imprescindible para garantizar el uso adecuado de las nuevas tecnologías artificiales.

Al respecto, de los principios éticos de IA se puede decir que existe una gran cantidad, pero existe cinco principios generales: "[B]eneficencia, No Maleficencia, Autonomía, Justicia y Explicabilidad".[138] Los principios éticos aplicados a la IA buscan

---

[133] "El soft law, aunque no constituye una fuente formal de derecho, se trata de un principio material que influye en la evolución normativa. Algunos instrumentos como declaraciones, recomendaciones y principios universales permiten articular guías de carácter ético, que posteriormente nutren tratados vinculantes o normas consuetudinarias. La Declaración Universal de los Derechos Humanos es un ejemplo no vinculante, pero clave para el desarrollo de pactos internacionales; en contextos nacionales, el soft law puede operar como presión indirecta hacia la formalización de estándares que regulen las nuevas TIC como la IA y las diferentes creaciones digitales". Jersain Zadamig Llamas Covarrubias, Olivia Andrea Mendoza Enríquez y Mario Graff Guerrero, "Enfoques regulatorios para la Inteligencia Artificial (IA)", *Revista Chilena de Derecho* 49, nº 3 (2022): 10, doi:10.7764/R.493.2.

[134] Juan Morales Ordoñez, *Ética y Sociedad*, (Cuenca: Universidad del Azuay, 2008), 17-21.

[135] Mark Coeckelberg, *Ética de la inteligencia artificial* (Madrid: Ediciones Cátedra, 2021), 15-20.

[136] UNESCO Conferencia General, *Recomendación sobre la ética de la inteligencia artificial*, 23 de noviembre de 2021, art. 4, A/RES/41/36.

[137] Luciano Floridi, *Ética de la inteligencia artificial* (Barcelona: Herder, 2023), 144-50.

[138] Ibíd., 146-52.

promover el bienestar y la dignidad humana mediante la beneficencia, evitar daños y proteger la privacidad a través de la no maleficencia, equilibrar la autonomía y la delegación de decisiones, garantizar la equidad en el acceso mediante la justicia, y exigir transparencia en los procesos tecnológicos a través de la explicabilidad.

Luciano Floridi, argumenta que "La ética no es, patrimonio de un solo continente o cultura. Cada empresa, agencia gubernamental o institución académica que diseñe o use IA tiene la obligación de hacerlo en consonancia con un marco ético".[139] El desarrollo de la IA tiene un impacto global, por tanto, el compromiso de cada organización ya sea gubernamental o privada, es desarrollar marcos éticos que promuevan valores universales. La ética de sistemas autónomos inició con Isaac Asimov en su obra de ciencia ficción denominada Circulo vicioso publicada en 1952.

Asimov, expuso las tres leyes de la robótica, que son las siguientes:

> "1. Un robot no debe dañar a un ser humano o, por su inacción, dejar que un ser humano sufra daño. […] 2. Un robot debe obedecer las órdenes que le son dadas por un ser humano, excepto cuando estas órdenes están en oposición con la primera ley. […] 3. Un robot debe proteger su propia existencia hasta donde esa protección no esté en conflicto con la primera o segunda ley."[140]

Las tres leyes de la robótica configuran un marco ético, bajo el que una entidad inteligente debería actuar para precautelar la vida e integridad del ser humano. Esta estructura se podría relacionar con el contrato social de Hobbes,[141] en este contrato los seres humanos pactan ceder su libertad a cambio de obtener seguridad. Así, las leyes de Asimov podrían considerarse el nuevo contrato social en la era digital. En el siglo XXI, el contrato social ya no gira únicamente en torno al individuo, sino a la reconfiguración de su libertad y seguridad al tener que compartir espacios con agencias inteligentes.

La aseveración de *agencia* que realiza el autor Floridi concibe que "[L]a inteligencia artificial no representa una inteligencia equivalente a la humana, sino a una nueva forma de agencia capaz de actuar, decidir y generar efectos en el mundo sin poseer

---

[139] Ibíd., 54-62.

[140] Adela Cortina, *¿Ética o ideología de la inteligencia artificial? El eclipse de la razón comunicativa en una sociedad tecnologizada* (Barcelona: PAIDÓS, 2024), 23-30.

[141] "Según Hobbes, el ser humano vive en un estado de naturaleza con libertad absoluta. Sin embargo, en este escenario surge la inseguridad y un permanente 'estado de guerra de todos contra todos', para asegurar su bienestar los individuos pactan un contrato social en el que ceden parte de su libertad, transfiriendo su poder de decisión a un soberano y a cambio de ello obtienen seguridad". Francisco Cortés Rodas, "El contrato social en Hobbes: ¿absolutista o liberal?", *Estudios Políticos del Instituto de Estudios Políticos de la Universidad de Antioquia* 5, nº 37 (2010): 1–15, doi: https://doi.org/10.17533/udea.espo.8072.

conciencia ni intención moral".[142] El autor mantiene una postura que concibe a la inteligencia de las máquinas como una nueva agencia o una nueva inteligencia diferente a la humana, además sostiene que esta herramienta aún no se ha perfeccionado para ser autónoma por completo y además tener consciencia de sus acciones.

Las plataformas digitales,[143] tales como Facebook, Instagram o WhatsApp son sitios de interacción social que han facilitado la difusión el contenido pornográfico. Por esta razón, resulta importante abordar la protección de los de derechos de las personas en estas plataformas, mediante las cuales se crea y comparte información de diferente índole. El compartir este tipo de contenido, no puede considerarse responsabilidad única las plataformas, ya que también debe analizarse la implementación de códigos éticos por parte de los desarrolladores y el adecuado manejo de los usuarios.

En relación al marco ético aplicado a las plataformas, se ha propuesto un conjunto de buenas prácticas en la distribución de contenido audiovisual entre las principales esta, "El respeto a los derechos de autor, la protección de la privacidad y la implementación de políticas y reglamentos".[144] Estas normas estan pensadas para contribuir con la seguridad de los datos personales. Sin embargo, es fundamental que las políticas de privacidad evolucionen hacia una ética activa, comprometida con el cuidado, la protección y la preservación responsable de la información.

El desarrollo de IA generativa se vincula con la responsabilidad de garantizar que sus creaciones respeten principios éticos. Esta aseveración invita a cuestionarse la capacidad de discernimiento ontológico de las máquinas, "Se trata, por tanto, de construir agentes morales artificiales capaces de seguir principios y tomar decisiones éticas".[145] Los algoritmos deben programarse bajo marcos éticos sólidos, para que, en la etapa de expansión, inicien a aprender de dichos datos para su funcionalidad y así evitar la transgresión con la creación y manipulación de contenido digital dañino.

En cuanto a los usuarios, podría relacionarse con la tercera ley de Asimov, basada en el cuidado y protección. La reflexión, se centra en los usuarios como destinatarios del

---

[142] Floridi, *Ética de la inteligencia artificial*, 68–73.

[143] "Las plataformas digitales son todos los sitios web como programas o aplicaciones en los que se recopila información de la empresa, así mismo los usuarios pueden acceder a las cuentas personales de contenido visual de textos, videos etc". Karina Lourdes Santistevan Villacreses, Johanna Lissette Arias Haro, y Sandy Briggette Sánchez Chávez, "Las plataformas digitales y su impacto en las ventas de las pequeñas empresas del cantón Paján", *Revista Estudios del Desarrollo Social: Cuba y América Latina* 8, nº 1 (2022): 6–15, doi:10.5281/zenodo.8383401.

[144] Alfabetización Audiovisual, "Ética Digital y Buenas Prácticas en la Producción y Distribución de Contenido Audiovisual", *Alfabetización Audiovisual*, accedido 18 de septiembre de 2025, párr. 5, https://roa.cedia.edu.ec/webappscode/135/tica_digital_y_buenas_prcticas.html.

[145] Cortina, *Ética o ideología de la IA*, 8–85.

producto digital dañino quienes, al difundir este tipo de contenido han vulnerado principios como el de no maleficencia,[146] al causar un perjuicio que podría haber sido evitable. En ese escenario, la educación digital es urgente no sólo para el uso adecuado de las herramientas digitales, sino también para dirigir a los usuarios hacía el discernimiento, la empatía y la defensa de los derechos fundamentales en entornos virtuales.

De esta manera, "La ética no sólo abarca principios generales, sino también incorpora nuevas dimensiones relacionadas con la alfabetización digital, la propiedad intelectual y la interacción en entornos virtuales".[147] La educación digital constituye una necesidad y debe ser impulsada por el Estado ecuatoriano, como condición básica para el ejercicio informado de la autonomía, entendida como la capacidad de decidir con conciencia y responsabilidad, requiere herramientas que permitan reflexionar críticamente en el tipo de creaciones que se genera y consume en el entorno digital.

Harari, en su libro *Nexus* afirma que "El dominio de la IA y de los datos podría permitir que los nuevos imperios se adueñaran de la atención de la gente".[148] Debe ejercerse el discernimiento frente al contenido digital que se consume, la atención de la humana es clave y puede ser medida mediante algoritmos. La ley cero de Asimov, menciona que "Un robot no puede dañar a la humanidad ni, por inacción, permitir que la humanidad sufra daño",[149] Es un principio que se refiere al bienestar colectivo, en el que la IA y las nuevas creaciones digitales son utilizadas para el bien común y no para causar daño.

---

[146] "Los principios clásicos serían el de beneficencia, que exigiría ahora poner los progresos al servicio de todos los seres humanos y la sostenibilidad del planeta; el de no maleficencia, que ordenaría evitar los daños posibles, protegiendo a las personas en cuestiones de privacidad, mal uso de los datos, en la posible sumisión a decisiones tomadas por máquinas y no supervisadas por seres humanos; pero también el principio de autonomía de las personas, que puede fortalecerse con el uso de sistemas inteligentes". Ibíd., 57.

[147] Tania Lisseth Rosado García et al., "Development of ethical values in digital education", *Universidad Ciencia y Tecnología* 29, nº 8 (2025): 3, doi: 10.47460/uct.v29iSpecial.885.

[148] Yuval Noah Harari, *Nexus: A Brief History of Information Networks from the Stone Age to AI* (Barcelona: Debate, 2024), 490-500.

[149] Cortina, *Ética o ideología de la IA*, 20–8.

Capítulo segundo
Desafíos en la regulación de *deepfakes* pornográficos

Estamos en un coche yendo hacia el
futuro, utilizando sólo nuestro espejo
retrovisor.
Herbert Marshall McLuhan.

1. Introducción al *hard law* en la regulación de la IA

La figura de la IA en los diferentes ámbitos de la vida social evidencia la necesidad de crear normas que regulen posibles riesgos derivados de esta nueva tecnología. El *hard law*,[150] entendido como el conjunto de normas obligatorias, es una herramienta para enfrentar los desafíos sociales que plantea los *deepfakes* pornográficos no consentido. A diferencia del *soft law*, basado en principios y recomendaciones sin carácter coercitivo,[151] el *hard law* busca establecer límites claros y garantías efectivas para la proteccion de los derechos fundamentales en el ciberespacio.

En un contexto digital sin protección resulta crucial sancionar toda forma de violencia digital que constituya una vulneración directa a la dignidad humana. Al abordar la legislación sobre IA, destaca la normativa creada por la Unión Europea, que ha avanzado significativamente en relación a otros países en este ámbito. En el año 2024, este bloque de países aprobó su primer marco normativo, conocido como el Reglamento 2024/1689 o *AI Act*,[152] en el cual establece las bases jurídicas para el desarrollo e implementación de los sistemas basados en IA.

La ley europea define los *deepfakes* o ultrasuplantaciones, como "[I]mágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación, que han sido generados o manipulados de manera artificial".[153] El reglamento establece que este contenido generado o manipulado a través de IA generativa, que simule ser auténtico debe

[150] "Instrumentos o prácticas generales con carácter obligatorio cuyo incumplimiento puede ser exigido por las vías instituciones de solución de conflictos y derivar en la responsabilidad internacional del Estado". Véase en Mauricio Iván del Toro Huerta, "El fenómeno del soft law y las nuevas perspectivas del derecho internacional", *Anuario Mexicano de Derecho Internacional* 1, nº 6 (2006): 5, doi:10.22201/iij.24487872e.2006.6.160.

[151] Guido Willians, *Conceptos de soft law, hard law, better regulation, smart regulation y políticas públicas* (Chile: Biblioteca del Congreso Nacional de Chile, 2021), 4-10.

[152] Unión Europea, *Reglamento de la Inteligencia Artificial (AI Act)*, 13 de junio de 2024, art. 1, A/RES/2024/1689.

[153] Ibíd., art. 3.

llevar una etiqueta clara y visible que advierta su naturaleza artificial. Asimismo, se prohíbe la difusión de *deepfakes* sin una indicación explícita de su origen, se ha llegado a una regulación debido al peligro de estas creaciones digitales sin un debido control.

Las plataformas digitales tienen la obligación de implementar mecanismos efectivos para reportar contenidos ilícitos y actuar con diligencia ante las denuncias recibidas. Los sistemas de IA en Europa han sido clasificados en cuatro niveles según el grado de riesgo que implican. A continuación, se muestra una gráfica que resume dicha clasificación:

Tabla 4

Riesgos de la IA según el reglamento europeo

Nivel de riesgo	Descripción	Ejemplos	Sanciones
Inaceptable	Su uso y desarrollo está prohibido de manera expresa por la UE. Sistemas de IA que constituyen una amenaza para derechos fundamentales y la dignidad humana.	Manipulación y explotación de vulnerabilidades. Puntuación social Vigilancia biométrica masiva *Deepfakes* pornográficos no consentidos	Multas de hasta 35 millones de euros o el 7% de la facturación global anual. Retiro del mercado y posibles procesos penales.
Alto riesgo	No están prohibidos, pero deben cumplir con parámetros de seguridad. Pueden impactar sectores clave como seguridad o salud.	IA aplicada en infraestructuras críticas. Sistemas masivos de identificación y vigilancia.	Multas de hasta 15 millones de euros o el 3% de la facturación mundial anual. Medidas de supervisión, auditoría y restricciones.
Riesgo limitado	Sistemas con riesgo potencial bajo. Requiere informar que el usuario interactúa con IA	Chatbots, asistentes virtuales, contenido multimedia generado por IA, siempre que sean identificados y consentidos.	Sanciones hasta 10 millones de euros y 2% de la facturación global.
Riesgo mínimo	IA sin riesgos o indicaciones especificas bajo el reglamento.	Filtros anti spam, video juegos, motores de búsqueda, etc.	Sin sanciones específicas.

Fuente: Reglamento 2024/1689 de inteligencia artificial de la UE[154]
Elaboración propia

En el marco de clasificación de riesgos, el nivel de riesgo inaceptable contempla usos prohibidos como la manipulación cognitiva o la vigilancia masiva. El riesgo alto está permitido únicamente bajo estricta regulación, especialmente en aplicaciones sensibles

[154] Ibíd., arts. 5, 8, 15, 29 y 50.
.

como la identificación biométrica. El riesgo limitado exige medidas de transparencia, aplicables a sistemas como *chatbots* o generadores de contenido. Finalmente, el riesgo mínimo no requiere restricciones, como ocurre en videojuegos que emplean IA, estos niveles determinan el tipo de sanciones y la libertad tecnológica.

Los *deepfakes* pornográficos se consideran de riesgo inaceptable, ya que vulneran derechos fundamentales de la persona. Su creación y difusión están prohibidas bajo, los desarrolladores y usuarios que incumplan esta norma pueden ser sancionados con multas de hasta 35 millones de euros o el 7 % de la facturación anual global, conforme lo establecido en el Reglamento,[155] de la UE. Asimismo, China destaca por haber implementado medidas para la Identificación del Contenido Sintético Generado por IA,[156] que busca reducir los riesgos del uso indebido de la IA y fomentar la innovación a través de valores socialistas.

El uso de *deepfakes* en China ya se regulaba; sin embargo, a partir de las medidas se prohibió su creación y difusión en casos de pornografía no consensuada. Además, se exige a los proveedores verificar la identidad real de los usuarios. De manera similar, en EE. UU. se ha regulado, a través de *Take it down act*[157] vigente desde el año 2025, se exige a las plataformas digitales eliminar el contenido sexual no consensuado en 48 horas tras el reclamo de la víctima, habilitando canales obligatorios para reportes. Los usuarios o plataformas, que difundan este material enfrentan sanciones penales y civiles.

A nivel internacional, los países firmaron el Convenio de Budapest,[158] reconocido como el primer instrumento jurídico para combatir la ciberdelincuencia en el contexto de las nuevas tecnologías. Este convenio ha sido clave para la evolución normativa en Europa, especialmente en materia de protección de datos y regulación de la IA. A diferencia de Latinoamérica, donde se denota la ausencia de armonización normativa a nivel regional, sumada al acelerado ritmo de avance tecnológico, dificulta la persecución de los delitos digitales que han traspasado fronteras jurisdiccionales.

Actualmente, este convenio cuenta con 75 países firmantes, entre ellos Brasil, México, Colombia y Ecuador. Estos estados, salvo Brasil, aún no han desarrollado

---

[155] Ibíd., arts. 5-99.

[156] China Briefing, "Comprender las nuevas regulaciones de China sobre IA generativa", *China Briefing News*, accedido 13 de julio de 2025, párr. 9, https://www.china-briefing.com/news/comprender-las-nuevas-regulaciones-de-china-sobre-ia-generativa/.

[157] Alonso Martínez, "Take it Down Act, la ley que criminaliza los deepfakes y la 'pornovenganza'", *El País US*, accedido 20 de mayo de 2025, párr. 2, https://elpais.com/us/2025-05-20/take-it-down-act-la-ley-que-criminaliza-los-deepfakes-y-la-pornovenganza.

[158] Consejo de Europa, *Convenio de Budapest contra la Ciberdelincuencia*, 23 de noviembre de 2001, art. 2, A/RES/94/185.

normativa en materia de IA, pero se encuentran en discusión varios proyectos de ley. La regulación es necesaria, particularmente en la creación y difusión de nuevos contenidos digitales dañinos, como los *deepfakes* pornográficos. Aunque no existe una normativa clara en esta materia, los mencionados países poseen leyes generales sobre la proteccion de datos y la sanción hacía delitos digitales.

A continuación, se presenta un mapa gráfico de las nomas principales:

Tabla 5
Análisis comparativo de la legislación latinoamericana

País	Ley de Protección de datos	Ley de delitos digitales	Proyectos de ley o leyes vigentes sobre regulación de IA y deepfakes pornográfico
Brasil	Ley general de protección de datos personales LGPD 2018.	Ley Carolina Dieckmann 2012.	Ley 2338/2023 sobre el uso de la inteligencia artificial de Brazil.
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares LFPDPPP última reforma 2025	Ley Olimpia reformatoria al Código Penal Federal	Proyecto de ley federal para el desarrollo ético, soberano e inclusivo de la IA.
Colombia	Ley 1581 (2012)	Ley 1273 reformatoria Código Penal de Colombia	Ley 2502 de 2025 que reforma art. 296 del Código Penal Proyecto de Ley 043 de 2025 para regular la inteligencia artificial
Ecuador	Ley Orgánica de Protección de Datos Personales	COIP	Proyecto de Ley Orgánica de Regulación y Promoción de la IA Proyecto de Ley de Fomento y Desarrollo de la IA Proyecto de Ley Orgánica de Aprovechamiento Digital e IA para Niñas, Niños y Adolescentes

Fuente: Alexandre Veronese & Amanda Nunes Lopes Espiñeira, Diário Oficial da União, Diario Oficial de la Federación, Diario Oficial de Colombia y Registro Oficial del Ecuador
Elaboración propia

En el caso de Brasil, este país cuenta con un sólido marco legal en protección de datos personales, como la Ley General de Protección de Datos Personales LGPD, [159] publicada en el año 2018 y el Marco Civil da Internet,[160] que refuerzan la privacidad digital y la protección de datos personales. La legislación brasileña reconoce conductas

[159] Brasil, *Lei Geral de Proteção de Dados Pessoais*, Diário Oficial da União, 14 de agosto de 2018, art.7.
[160] Brasil, *Marco Civil da Internet*, Diário Oficial da União 12.965, 23 de abril de 2014, art. 9.

como la difusión no autorizada de imágenes íntimas a través de la Ley Carolina Dieckmann,[161] vigente desde el año 2013, promovida en base al caso de la actriz homónima, cuyas fotos íntimas fueron robadas y divulgadas sin consentimiento.

El senado brasileño discute propuestas enfocadas a prevenir la violencia digital; especialmente contra menores. Así como, el Proyecto De Ley 2338/2023[162] sobre el uso de IA, aunque no se sanciona las creaciones digitales íntimas no consentidas, contempla medidas para la protección de derechos frente al mal uso de las TIC. México y Colombia, han desarrollado marcos legales sólidos para la protección de datos personales, aunque con enfoques distintos. En México, de la Ley Federal De Protección De Datos Personales En Posesión De Los Particulares[163] del año 2025, prioriza los derechos ARCO[164] de los titulares de datos personales.

Por otro lado, Colombia aborda la proteccion de derechos personales a través de la Ley Estatutaria Nº 1581[165] del año 2022 y el Convenio de Budapest[166] articulando la protección de datos con estándares internacionales. En materia de delitos digitales, los dos países reconocen la violencia digital y tipifican conductas lesivas en contra la intimidad e indemnidad. En el caso de México, la Ley Olimpia[167] trata de un conjunto de reformas legislativas que sanciona la difusión no consentida de contenido íntimo. Al igual que este país, Colombia cuenta con la Ley 1273,[168] que protege el derecho a la intimidad e indemnidad de las personas.

Respecto a la regulación de IA, ambos países presentan vacíos normativos; México, apenas inicia propuestas legislativas, mientras que Colombia muestra avances concretos, con proyectos que abordan el uso malicioso de *deepfakes* en contextos sexuales no consentidos. Por otro lado, la Ley 2502,[169] de 2025 reforma artículo 296 del Código Penal Colombiano, cuya vigencia iniciará a partir del año 2026 y su objetivo fundamental es tipificar una agravante de suplantación mediante IA incluyendo el uso de *deepfakes*.

---

[161] Brasil, *Ley Carolina Dieckmann*, Diário Oficial da União 12.737, 3 de diciembre de 2012, art. 154-A.

[162] Brasil, *Projeto de Lei nº 2338/2023*, Diário Oficial da União 2338, 3 de mayo de 2023, art.6.

[163] México, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Diario Oficial de la Federación, 21 de marzo de 2025, art.22.

[164] México, *Guía para el ejercicio de los derechos ARCO*, Sitio web institucional INAI, 6 de enero de 2012.

[165] Colombia, *Ley Estatutaria para la Protección de Datos Personales*, Diario Oficial de la República, 18 de octubre de 2012, art. 9.

[166] Consejo de Europa, *Convenio de Budapest contra la Ciberdelincuencia*, arts. 2,5,6,14 y 18.

[167] México, *Ley Olimpia*, Diario Oficial de la Federación ,2 de junio de 2021, art. 6.

[168] Colombia, *Ley 1273*, Diario Oficial de la República, 5 de enero de 2009, art. 269A.

[169] Colombia, *Ley 2502*, Diario Oficial de la República, 28 de julio de 2025, art. 3.

Además, existe el proyecto de ley 043[170] de 2025 que propone establecer un marco normativo para la regulación de la IA en Colombia.

Finalmente, Ecuador en materia de protección de datos personales el país cuenta con la Ley Orgánica de Protección de Datos Personales,[171] vigente desde 2021 aunque su aplicación práctica y régimen sancionador son aún limitados; la ley establece principios de consentimiento, transparencia y protección de datos sensibles. El Código Orgánico Integral Penal COIP[172] (en adelante COIP) vigente desde el año 2014, tipifica delitos informáticos como la pornografía infantil o la difusión de contenido íntimo no autorizado.

Aunque, aún no se ha regulado o tipificado a los *deepfakes* pornográficos como un delito, la regulación de IA se encuentra en fase de discusión legislativa de tres proyectos de ley con énfasis en proteger los derechos fundamentales y promover la innovación. En su texto integral los proyectos de ley no mencionan explícitamente los *deepfakes,* su enfoque se centra en la regulación de sistemas de alto riesgo, como el reconocimiento facial y la toma de decisiones automatizadas lo cual podría constituir una base inicial para incorporar esta tecnología en el marco legal.

Figura 5. A la derecha, ejemplo de una imagen editada con el programa de IA Grok, de X., 2026
Fuente: Plataforma Digital El País[173]

[170] Colombia, *Proyecto de Ley para regular la IA Colombia*, Proyecto de ley 043, 30 de julio de 2025, art.12.

[171] Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, 18 de octubre de 2012, art. 1.

[172] Ecuador, *Código Orgánico Integral Penal COIP*, arts. 103, 178 y 230.

[173] Diario El País, "El escudo legal frente a los 'deepfakes' sexuales: los desnudos generados con IA van más allá de Grok", *Diario El País*, accedido 14 de enero de 2026, https://n9.cl/g1nz3.

1.1. Procedimiento administrativo y *deepfakes* pornográficos

Para iniciar, es necesario aclarar que no existe una vía de solución ya sea administrativa o judicial, que sirva al abordar el problema de los *deepfakes* pornográficos. Sin embargo, en los casos concretos del presente estudio, la afectación se origina en el ámbito institucional de carácter educativo, por ello se tratará de explicar la forma en que dicha instancia debió actuar. En primer lugar, en el caso de Sofía, la violencia digital inició en su lugar de estudios, es decir, en el mismo establecimiento educativo que debía garantizarse la protección a sus derechos.

Según la CRE, el Estado y sus funcionarios son los principales garantes del ejercicio efectivo de los derechos fundamentales. Así, "El ejercicio de los derechos se regirá por los siguientes principios: […] 9. El más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución".[174] El Estado, tiene el deber de garantizar y hacer cumplir los derechos de los administrados, es decir, la población ecuatoriana. En casos de vulneraciones, se aborda la vía administrativa, en la propia institución educativa dedicada a tal fin.

En base al concepto formulado por el destacado jurista Roberto Dromi, sostiene que; "El procedimiento administrativo es el instrumento jurídico por el que se viabiliza el actuar de la relación administrado-administración. […] articula, regula y a la vez habilita el ejercicio de las prerrogativas públicas que integran el poder",[175] constituye la vía por medio de la cual la administración manifiesta su voluntad y se trata de una herramienta que garantiza el respeto de los derechos para las personas que se someten a dicho procedimiento. No es meramente técnico, sino también una forma de protección y defensa, a la que puede acogerse el administrado en este caso las víctimas.

En el caso concreto, representa el camino que debe seguir Sofía y su madre María para esclarecer los hechos ocurridos, al igual que Simón. De esta manera, el Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación,[176] ha establecido la vía administrativa idónea, frente a situaciones de violencia virtual. En el primer caso la persona en tener conocimiento fue el docente tutor, a partir de este hecho según el Protocolo, se activa el procedimiento institucional, con la notificación del docente a la autoridad competente del plantel.

---

[174] Ecuador, *Constitución de la República del Ecuador*, art. 11, núm. 9.

[175] Roberto Dromi, *Derecho Administrativo* (Lima: Gaceta Jurídica, 2005), 891-5.

[176] Ecuador Ministerio de Educación, *Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación*, MINEDUC-2023-00054-A, 21 de septiembre de 2023, arts. 1, 2, 3 y 4.

El rector, como máxima autoridad de la institución, así como los padres de los estudiantes y el Departamento de Consejería Estudiantil (DECE), deben realizar una adecuada contención emocional, es decir tratar de conectar con la víctima. Y posteriormente, proceder a elaborar una ficha que sería la denuncia formal, señalando el motivo, los primeros signos de alerta y las acciones ya tomadas. En el Protocolo se ha denominado, diagnóstico situacional porque considera la esfera individual, familiar y grupal en corresponsabilidad con el proceso psicoeducativo, dicho enfoque es urgente frente a estos casos de *deepfakes* pornográficos.

En casos particulares no sólo se debe analizar los impactos sociales y emocionales, sino también las rutas de reparación, generando un espacio en el que los padres y los estudiantes, consideran a través de un consentimiento informado, la atención psicosocial, que incluye el plan de trabajo y los compromisos de ambas partes. Al constatar que se trata de un posible ilícito, la entidad debe denunciar ante la Fiscalía, no se podía iniciar una investigación formal, debido a que, "No hay infracción penal, pena, ni proceso penal sin ley anterior al hecho".[177] al no estar tipificada la creación y difusión de contenido pornografico a través de IA, no se podía sancionar.

El art. 206 lit. a del Código de la Niñez y Adolescencia, establece las atribuciones de las Juntas de Proteccion de Derechos Humanos, como "Conocer, de oficio o a petición de parte, los casos de amenaza o violación de los derechos individuales de niños, niñas y adolescentes dentro de la jurisdicción del respectivo cantón; y disponer las medidas administrativas de protección que sean necesarias para proteger el derecho amenazado o restituir el derecho violado".[178]

Al no existir una vía penal de juzgamiento, la Fiscalía debió emitir el archivo y derivar la causa a la Junta Cantonal de protección de Derechos, la misma al conocer de este suceso debe abrir un expediente administrativo,[179] seguidamente debe dictar medidas inmediatas de protección, como atención psicológica urgente a las víctimas, protección, acompañamiento y tratar de eliminar el contenido dañino, para ello la Junta debe colaborar con otras instituciones como Fiscalía, DECE o Defensoría del Pueblo.

Los teléfonos interceptados resultan indicios, para que se pueda investigar e imponer las sanciones necesarias que estime la Junta y si resultan insuficientes la Junta

[177] Ecuador, *Código Orgánico Integral Penal COIP*, art. 5.1.
[178] Ecuador, *Código de la Niñez y Adolescencia*, art. 206, lit. a.
[179] "[...] Mantener expedientes completos y actualizados de cada niño, niña o adolescente [...]". Véase en Ecuador, *Código de la Niñez y Adolescencia*, art. 211 lit. n.

debe recurrir a instancias judiciales como la derivación del caso a Unidad Judicial Especializada en Familia, Mujer, Niñez y Adolescencia o a la Defensoría del Pueblo, desde el punto de vista administrativo, los adolescentes que presuntamente fueron responsables de este hecho, tras un procedimiento administrativo, debieron afrontar medidas sancionatorias, en la institución educativa y por parte de Junta Cantonal.

En el segundo caso, como abogado y académico la trayectoria de Simón personal y profesional fue afectada. El abordaje inicial debió ser a través de las autoridades educativas, dado que los hechos ocurrieron en el entorno institucional. En este marco correspondía la apertura de un expediente administrativo, identificando el hecho como la forma de violencia digital en contra del docente. Dicha denuncia debía ser tramitada a través del Departamento Jurídico o conforme a los protocolos internos que maneje dicha institución de Educación Superior.

La potestad de juzgar que mantiene la universidades, se sustenta en la Constitución, que reconoce la autonomía institucional, manifestando que "El Estado reconocerá a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución".[180] Facultando a las universidades para normar y sancionar conductas que vulneren los derechos de estudiantes y docentes, como el caso concreto de violencia digital, en contra del docente.

El expediente administrativo sirve para mantener las evidencias, de las mismas se deriva los argumentos jurídicos y una posible solución. Aunque en Ecuador no existe una homogeneidad, en casos de violencia digital suscitados a docentes o estudiantes. La autoridad instructora al dar inicio al procedimiento administrativo, debe guiarse por los principios comunes a este procedimiento establecidos en la CRE y Código Orgánico Administrativo (en adelante COA), como la imparcialidad.

El jurista Andrés Moreta, menciona que "[E]l funcionario público no tenga un conflicto de interés, este principio se plasma en el procedimiento administrativo sancionador al establecerse en el art. 248 núm. 1 como una de sus garantías la separación entre órgano instructor y resolutor".[181] La imparcialidad, es importante dado que la violencia digital debe investigarse evitando cualquier presunción de culpabilidad. En ese

[180] Ecuador, *Constitución de la República del Ecuador*, art. 355.

[181] Andrés Moreta, *Procedimiento Administrativo y Sancionador en el COA* (Quito: Ediciones Continente, 2019), 10.

sentido, se exige una separación entre el órgano instructor que se encarga de conducir la investigación y el órgano resolutor que debe emitir la resolución.

A continuación, se presenta una sistematización de las posibles infracciones administrativas atribuibles a los servidores públicos de instituciones educativas de nivel secundario y superior, en el marco de su deber funcional de prevención, actuación y reparación frente a situaciones de violencia digital, conforme a los principios de protección integral y corresponsabilidad institucional.

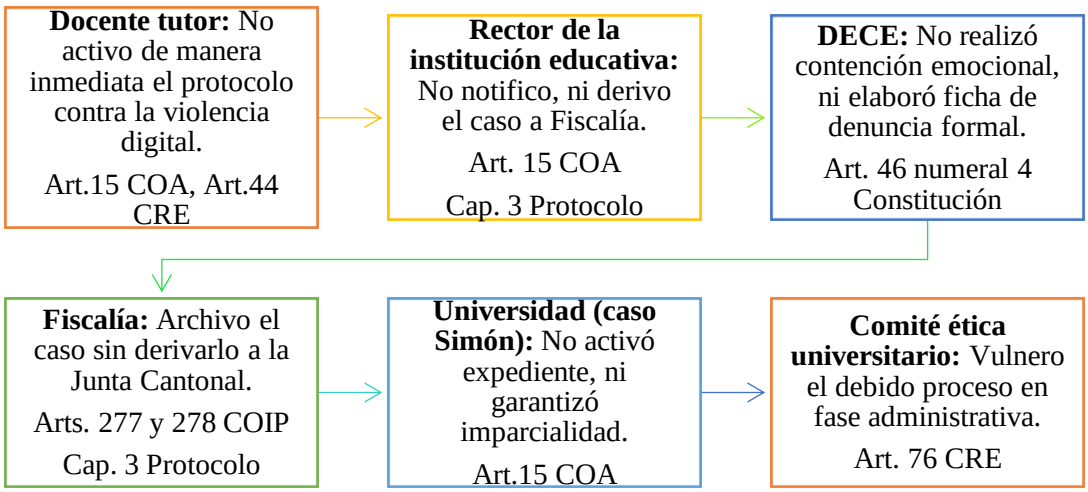


Figura 6. Infracciones administrativas cometidas por servidores públicos
Fuente: Adaptado del testimonio de Sofía y Simón (seudónimos), CRE, COA, COIP y Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación[182]

Las infracciones vulneraron derechos como la dignidad, la intimidad, la protección frente a la violencia digital y el acceso a reparación, en la fase administrativa, la reparación integral como derecho está consagrada en la CRE ecuatoriana,[183] que obliga a los funcionarios del Estado a respetar y hacer respetar los derechos vulnerados. El COA, establece la reparación en sede administrativa, en ambos casos, debió activarse ante la falta de respuesta penal, así ambos debieron acceder a protección y restitución de sus derechos, desde sus respectivas entidades educativas.

1.2. Reparación civil: reconocimiento del daño moral y patrimonial

La afectación provocada por contenidos digitales no consentidos, como los *deepfakes* de índole sexual vulnera la dignidad humana. El derecho civil, contempla

[182] Ecuador, *Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación*, cap. 3.
[183] Ecuador, *Constitución de la República del Ecuador*, art. 11 numeral 9 y 75.

mecanismos de reparación para restituir en medida de lo posible, la situación anterior al daño. La acción por daños y perjuicios permite reclamar el daño emergente y el lucro cesante, en nuestra legislación ecuatoriana el daño y el perjuicio son términos que suelen emplearse como equivalentes, pero la doctrina establece la separación entre ambos conceptos.

Según el autor José García Falconí, "El daño es el género y el perjuicio la especie, el daño se puede entender como el mal padecido por una persona o causado en una cosa y el perjuicio es la ganancia o beneficio, cierto o positivo que ha dejado de obtenerse".[184] En tal sentido, la obligación civil de reparar se trata de resarcir los perjuicios ocasionados a otra persona ya sea capaz o incapaz conforme ha señalado la legislación civil. Dicha reparación, no solo constituye un mecanismo jurídico, sino una garantía para alcanzar la justicia y la restitución.

El Código Civil ecuatoriano, en materia de indemnización de daños y perjuicios, establece que, "comprende el daño emergente y el lucro cesante, ya sea que provengan de no haberse cumplido la obligación, o de haberse retardado el cumplimiento".[185] A partir de la normativa y la doctrina civil, se ha determinado que existen dos clases de daño: patrimonial y extrapatrimonial. El primero concibe el daño emergente y el lucro cesante; el segundo, el daño moral.

En el caso concreto del daño moral, debe "Ser evaluado en forma separada del daño patrimonial, el juez no debe estimar el daño moral en porcentaje del daño patrimonial".[186] El daño patrimonial puede llegar a repararse, dado que es susceptible de ser evaluado y cuantificado. En contraste, al daño extrapatrimonial vinculado al daño moral que sufre la persona que por su naturaleza subjetiva no puede cuantificarse dada la afectación a la esfera psicológica y emocional del individuo, por tal razón su estimación queda confiada a criterio del juez.

En relación al daño moral, se entiende "Como un detrimento de carácter psicológico y mental que afecta a la estima social, la identidad, dignidad del que lo soporta".[187] En casos de violencia digital el deterioro puede infligirse en la esfera

---

[184] José Carlos García Falconí, *La demanda civil de daños y perjuicios y daño moral por responsabilidad subjetiva en contra de los jueces, fiscales y defensores públicos* (Quito: Ediciones Rodin, 2010), 204-10.

[185] Ecuador, *Código Civil*, Registro Oficial 46, Suplemento, 24 de junio de 2005, art. 1572.

[186] García Falconí, *La demanda civil de daños y perjuicios y daño moral por responsabilidad subjetiva en contra de los jueces, fiscales y defensores públicos*, 207-15.

[187] José Sánchez Zambrano, Inés Guamán Lema, y Pedro Peñafiel Fárez, "Daños y Perjuicios y Daño Moral en el Sistema Procesal Ecuatoriano", *Derecho Crítico: Revista Jurídica, Ciencias Sociales y Políticas* 8, nº 3 (2023): 9, doi:10.53591/dcjcsp. v3i3.1095.

psicológica y emocional de la persona. Los *deepfakes* pornográficos, vulneran la intimidad, provocan dolor y tristeza en la persona; aunque el hecho no ocurra físicamente, el impacto emocional es similar a una agresión tangible que puede provocar despidos como el caso de Simón; y estigmatización como ocurrió con Sofía.

La legislación civil ecuatoriana, prevé lo siguiente:

> La acción por daño moral corresponde exclusivamente a la víctima o a su representante legal. Mas, en caso de imposibilidad física de aquella, podrán ejercitarla su representante legal, cónyuge o parientes hasta el segundo grado de consanguinidad. De haber producido el hecho ilícito la muerte de la víctima, podrán intentarla sus derechos habientes, conforme a las normas de este Código. Cuando el daño moral afecte a las instituciones o personas jurídicas, la citada acción corresponderá a sus representantes.[188]

En el caso de Sofía y su madre María en calidad de representante legal tiene la potestad de interponer la acción civil por daño moral. Por el contrario, Simón puede ejercer la acción por sus propios derechos. Es importante destacar que la legislación reconoce a las personas jurídicas, aunque las mismas carecen del aspecto emotivo por su naturaleza, poseen derechos extrapatrimoniales como el honor, la reputación y el buen nombre. Por ello, al verse afectadas también podrían demandar dicha vulneración y exigir la compensación por daño moral.

Para determinar la indemnización de daño moral, la autora Daniela Páez, distingue dos categorías:

> La pecunia doloris (precio del dolor) engloba dos aspectos diferentes: el dolor físico que la víctima experimenta como consecuencia del hecho dañoso sobre su propio cuerpo, que incluye las sensaciones de malestar, el insomnio o cualquier tipo de manifestación dolorosa que se haya originado en su disminución física, y; el puro daño moral, representado por el dolor moral que se refleja en la pena, la tristeza y el sufrimiento no físico, que pueden padecer tanto la víctima directa como sus parientes.[189]

En el caso de daño físico; los *deepfakes* pornográficos el cuerpo de la víctima no es violentado materialmente, sino a través de las alteraciones digitales. Por tanto, no se configura un daño físico directo, pero sí emerge un daño moral como lo señala la autora perceptible en la pena, la tristeza, la vergüenza y desesperación que siente la víctima. Ese sufrimiento, se extiende a las personas más cercanas a su entorno afectivo siendo su familia, su comunidad, los jefes, los compañeros de trabajo, los docentes y los compañeros y compañeras de estudios.

---

[188] Ecuador, *Código Civil*, Registro Oficial 46, Suplemento, 24 de junio de 2005, art. 2233.

[189] Daniela Páez Salgado, "¿Daño moral por incumplimiento de contrato?", en *Iuris Dictio* 14, nº 16 (2015): 4, doi:10.18272/iu. v14i16.729.

Para cuantificar el daño moral, "Josserand un influyente jurista francés, se refiere al *pretrium doloris*, como el padecimiento, la congoja, el dolor que sufre la víctima o cualquier persona relacionada con él que cargue con tal sentimiento, que será indemnizado según el arbitrio judicial".[190] El *petrium doloris*, se traduce como el precio del dolor, y alude a la compensación económica que le corresponde a una persona por los sufrimientos morales padecidos, considerándose un precio razonable y justo aunque a pesar de ello existe la discusión que no hay precio que pueda compensar el dolor.

Respecto al resarcimiento de daño moral, la autora María del Socorro, menciona:

> La doctrina considera que el dinero es un instrumento viable para la indemnización del daño moral, aunque no haya correspondencia valorativa con el propio dinero, se crea una fuente de satisfacción frente al daño causado. Se ha incurrido en un error, cual es considerar que la indemnización dada por el dinero a título de daño moral, no hace desaparecer, ni atenúa el efecto generado al bien moral que se lesiona. Con el dinero se puede mitigar el dolor.[191]

Aunque el daño moral no puede ser reparado, en la práctica se reconoce que la indemnización, si bien no anula el sufrimiento, puede mitigar sus efectos. En casos de *deepfakes* pornográficos, las víctimas enfrentan una vulneración de sus derechos íntimos y personales, agravándose por la omisión institucional. El daño más que corporal es moral, una falsificación de la imagen que atenta contra la dignidad, ante este vacío la compensación económica pretende ser un gesto reparador y aunque pueda resultar insuficiente, pretende reconocer el dolor padecido y atenuarlo.

En cuanto a la fijación, de la cantidad resarcitoria la jurisprudencia, sin embargo, se ha propuesto que "El juez debe fijarlo, ajustando a la prudencia y equidad, esto es de manera razonable y equitativa con arreglo al mérito probatorio aceptable que arroja el proceso".[192] En el juicio por daño moral corresponderá al juez, establecer el monto adecuado en base a las pruebas presentadas por las partes especialmente por la víctima que pretende obtener la reparación. La cantidad que se fije no es una fuente de enriquecimiento sino una medida de reconocimiento del dolor, ante el daño causado.

La Constitución, en base a la reparación ha establecido, que "[L]a jueza o juez resolverá la causa mediante sentencia, y en caso de constatarse la vulneración de derechos

---

[190] María del Socorro Rueda Fonseca, "Las Vertientes Doctrinarias Del Daño Moral o Petrium Doloris", *Revista Boliviana de Derecho* 10, nº 4 (2007): 20, http://www.redalyc.org/articulo.oa?id=427539904003.

[191] Ibíd., 17.

[192] García Falconí, *La demanda civil de daños y perjuicios y daño moral por responsabilidad subjetiva en contra de los jueces, fiscales y defensores públicos*, 237-45.

deberá declararla, ordenar la reparación integral, material e inmaterial, y especificar e individualizar las obligaciones, positivas y negativas, a cargo del destinatario de la decisión judicial, y las circunstancias en que deban cumplirse".[193] La reparación integral, según el art. 86 núm. 3 de la CRE, establece la restitución, la rehabilitación, la satisfacción simbólica y las garantías de no repetición.

La reparación integral se basa en restaurar la dignidad humana vulnerada por la transgresión de derechos fundamentales. En el contexto de los *deepfakes* pornográficos no consentidos, el daño moral exige una respuesta que mediante una sentencia de carácter constitucional se reconozca y restituya. Ante la ausencia de esta reparación, se podría demandar a través de la vía civil. Esta acción no solo busca compensar el perjuicio, sino también visibilizar la violencia simbólica ejercida mediante tecnologías emergentes.

En la esfera patrimonial, es necesario reconocer que los *deepfakes* pornográficos pueden afectar derechos patrimoniales, en el caso de Simón Rivas, menciona: "Aunque no parezca, ese episodio terminó afectando mi carrera, tenía posibilidades reales de ser decano".[194] Existió daño emergente ante la salida precipitada de la universidad; dejando de percibir el sueldo como docente, y lucro cesante ante un posible ascenso que no se concretó, lo que implica pérdida de ingresos, estabilidad laboral y prestigio académico, resultando difícil trabajar en otras universidades o instituciones.

La cantidad debe tazarse en relación al daño, Zavala Egas et al. mencionan que "[S]i se ha litigado sobre la especie y el monto de los perjuicios, el que los cobra debe acreditar dicha especie y monto".[195] Los requisitos fundamentales para acceder a la indemnización es la demanda por daños y perjuicios, en donde corresponde al demandante asumir la carga de la prueba y demostrar que dicho daño se produjo. La prueba debe consistir en elementos, que acrediten la salida precipitada de la universidad, como por ejemplo el expediente administrativo del docente.

A continuación, se presenta un esquema organizacional que facilita la comprensión de las rutas de actuación, desde el enfoque civil y administrativo:

---

[193] Ecuador, *Constitución de la República del Ecuador*, art. 86.

[194] Simón Rivas, entrevistado por la autora, 15 de julio de 2025. Para leer la entrevista completa, ver Anexo 3.

[195] Jorge Zavala Egas et al., *Homenaje Póstumo al Dr. Edmundo Durán Díaz* (Quito: Universidad hemisferios, 2002), 90-5.

Tabla 6
Enfoque civil y administrativo respecto a los deepfakes pornográficos

Dimensión	Administrativo	Civil
Naturaleza jurídica	Público	Privado
Procedimiento	Procedimiento administrativo, protocolos internos y medidas de protección	Juicio ordinario por daños y perjuicios
Normativa aplicable	COA, Código de la Niñes y Adolescencia y Protocolos Educativos	Código Civil, Doctrina nacional y comparada
Actores involucrados	Instituciones educativas, DECE, Juntas de Protección y Defensoría del Pueblo	Juez de lo Civil y Mercantil, demandado y demandante
Finalidad	Medidas administrativas, atención psicológica, eliminación de contenido	Indemnización por daño emergente, lucro cesante y daño moral
Limitaciones	No impone sanciones civiles como indemnizaciones económicas	No garantiza contención emocional ni medidas institucionales inmediatas

Fuente: COA, Código Civil, Protocolo en casos de violencia digital, Roberto Dromi[196] y José Carlos García Falconí et al.[197]
Elaboración propia

2. Desafíos constitucionales: garantía de la dignidad humana y derechos digitales

Los derechos fundamentales y la dignidad no deben entenderse como meros enunciados, sino como una herramienta para enfrentar los desafíos de esta nueva realidad marcada por el avance de la IA y los *deepfakes* pornográficos, como prácticas que deshumanizan a la persona y socavan los derechos fundamentales. En este acápite, se presenta un análisis detallado de los principales derechos y su afectación, trazando un recorrido desde una perspectiva convencional hacia el cambio de paradigma que exige una reinterpretación en el marco de los derechos digitales.

Para iniciar, los derechos digitales se entienden como garantías que protegen a los ciudadanos en el entorno digital y abarca:

> Los derechos de los ciudadanos en el entorno digital, ya sean derechos fundamentales o derechos ordinarios. Esta categoría es especialmente relevante porque la transformación digital debe tener como principio estructural maximizar la calidad de la democracia y los derechos. […] lo que plantea el problema de cómo protegerlos adecuadamente dadas las especiales características del mundo digital.[198]

[196] Dromi, *Derecho Administrativo*, 405–70.
[197] García Falconí, *La demanda civil de daños y perjuicios y daño moral por responsabilidad subjetiva en contra de los jueces, fiscales y defensores públicos*, 47–80.
[198] Moisés Barrio Andrés, "Génesis y desarrollo de los derechos digitales", *Revista de las Cortes Generales* 6, nº 10 (2021): 11, doi:10.33426/rcg/2021/110/1572.

Los derechos digitales, están orientados a proteger la dignidad de la persona en el entorno digital, incluyendo los derechos fundamentales, siendo que la vida digital no es ajena a la realidad, si no que ya es parte de la vida cotidiana. La dignidad humana constituye el punto de partida de dichos derechos, el tratadista Manuel Atienza, sostiene que la dignidad "Implica el deber de respetar el libre desarrollo de las demás personas".[199] Dado que cada persona tiene la facultad de actuar con autonomía personal, siempre que respete los límites de los derechos de los demás.

Por otro lado, el autor Hernán de León entiende a la dignidad humana como "El derecho que tiene cada uno de ser valorado como sujeto individual y social, en igualdad de circunstancias".[200] Haciendo referencia a la persona, como ser capaz de decidir sobre su propia vida. Incorporando la dimensión social, que reconoce al individuo en relación con otros, sin perder su individualidad. Según, la DUDH,[201] "Todos los seres humanos nacen libres e iguales en dignidad y derechos",[202] subrayando el carácter innato de la dignidad como condición humana, se trata de la capacidad de valorarse a sí mismos en la dimensión individual y social.

En la sentencia Nro. 001-10-PJO-CC la Corte Constitucional del Ecuador señala que "La dignidad humana es el valor supremo que informa todo el ordenamiento jurídico; su respeto y garantía constituyen el fundamento de los derechos".[203] La Corte, establece que la dignidad no depende de condiciones externas como la edad, la orientación sexual o la situación jurídica, sino que es inherente a la persona por el hecho de ser humana, lo que implica que cualquier afectación a la imagen o reputación como ocurre con los *deepfakes* pornográficos constituye una violación constitucional directa.

La Corte Constitucional, ha establecido que la dignidad es el valor supremo del orden jurídico en la sentencia No. 001-10-PJO-CC, y que su respeto constituye el fundamento de todos los derechos. En las sentencias No. 2539-18-EP/24[204] y la No. 2063-17-EP/22[205], de la Corte se fortalece la protección de la dignidad e imagen frente a las diferentes formas de violencia. En la primera, se discutió el uso no autorizado de

[199] Manuel Atienza, *Sobre la dignidad humana* (Madrid: Trotta, 2022), 12-18.

[200] Hernán Antonio León Batista, "La dignidad humana en la era digital", *Anuario de Derecho Constitucional Latinoamericano* 26, nº 8 (2020): 2, https://biblio.juridicas.unam.mx/bjv.

[201] ONU Asamblea General, *La Declaración Universal de los Derechos Humanos*, preámbulo.

[202] Ibíd., art. 1.

[203] Ecuador Corte Constitucional, "Sentencia", en *Juicio n.º: 001-10-PJO-CC*, 22 de diciembre de 2010, párr. 4.

[204] Ecuador Corte Constitucional, "Sentencia", en *Juicio n.º: 2539-18-EP/24*, 01 de agosto de 2024, párr. 54.

[205] Ecuador Corte Constitucional, "Sentencia", en *Juicio n.º: 2063-17-EP/22*, 27 de julio de 2022, párr. 63.

personajes televisivos, y aunque se declaró improcedente la vía constitucional para resolver controversias patrimoniales, se extendió el derecho a la imagen.

La sentencia No. 2063-17-EP/22, reconoció la vulneración de la imagen y presunción de inocencia de un ciudadano expuesto mediáticamente, sin sentencia ejecutoriada. La Corte ordenó reparación y exhortó a los medios a respetar estándares éticos en la difusión de información. Esta sentencia, junto con la sentencia No. 2539-18-EP/24, que abordó el uso no autorizado de personajes televisivos, refuerza la protección constitucional de la imagen, permitiendo enfrentar fenómenos como los *deepfakes* pornográficos incluso sin normativa específica previa.

La dignidad humana trasciende su concepción tradicional para ser reinterpretada constitucionalmente. Algunas acciones llevadas a cabo, "La exposición no consentida, la manipulación de la imagen y la circulación de contenidos degradantes, exigen repensar la dignidad como un derecho activo, cuya protección se extiende al espacio virtual, más allá de la integridad física".[206] La dignidad humana, que ha sido objeto de protección en la esfera tangible, enfrenta nuevos desafíos en el entorno digital. En esta nueva era, los datos personales se han convertido en el principal activo.

Por tanto, su protección exige una especial atención al entorno digital, los *deepfakes* pornográficos como una expresión dañina se originan en el mal uso de la tecnología y generan transgresión a los derechos en entornos virtuales, la revolución digital y la sociedad de la información, reafirma:

> El reconocimiento de varios derechos digitales, como: el derecho existir digitalmente, el derecho a la identidad digital, la reputación digital, el derecho de acceso a internet, la protección de datos y la participación digital. […] cada ola de derechos humanos responde a las necesidades y demandas de cada época histórica, y que no supone la sustitución o la negación de las olas anteriores, sino su complementación y su ampliación, pues son un proceso dinámico y progresivo.[207]

La cuarta revolución tecnológica no solo impulsa el avance digital y las condiciones de interacción social, sino que genera nuevos derechos, tales como la autodeterminación informativa, el derecho al olvido, el derecho a la seguridad e identidad digital, inclusive derechos como la desconexión o la educación digital. Todos estos nuevos derechos se han amplificado para crear la posibilidad de ejercer los derechos

[206] León Batista, "La dignidad humana en la era digital", 22-5.

[207] Lorena Naranjo Godoy, "Aproximación a la categorización de derechos digitales y su aplicación en Ecuador", *Revista Cálamo* 5, nº 21 (2024): 7, doi:10.61243/calamo.21.423.

clásicos en el entorno digital, evitando discriminaciones, protección especial de la persona y su participación en la red.

Uno de los derechos más importantes de esta nueva oleada se trata del derecho de acceso universal a internet.[208] En el mundo de grandes desarrollos tecnológicos, el internet constituye la base para acceder a la web y entender el significado de ciertos derechos ya conocidos, tales como: la identidad, intimidad, integridad o la privacidad y los nuevos derechos emergentes. De esta manera, al igual que la tecnología el derecho no puede ser estático, sino que debe responder a las nuevas demandas y adaptarse a la evolución de la sociedad, siendo esta una sociedad digitalizada.

Profundizando en el análisis de las posibles vulneraciones derivadas del uso de las TIC en particular de la IA y sus creaciones digitales. El autor, Miguel Ángel Presno, señala que:

> Parece que entre los derechos fundamentales más afectados por el uso de sistemas IA estarán los que garantizan la dimensión privada de las personas: la intimidad, la propia imagen, la protección de los datos personales y el secreto de las comunicaciones […] y es que uno de los factores que convierten a la IA en una herramienta tan poderosa es su capacidad para el tratamiento de una ingente cantidad de datos.[209]

La mayor vulneración ante el avance de la IA se relaciona con los derechos personales. Estos derechos se vinculan con los datos personales, que, en el entorno digital, circulan en grandes volúmenes y se encuentran al alcance público. En un mundo hiperconectado,[210] lo que caracteriza a esta nueva realidad es la facilidad que estos datos pueden ser identificados, extraídos y utilizados. La IA, se nutre de ellos, en su procesamiento y puede dar lugar a creaciones significativas, pero también a vulneraciones profundas de derechos.

La UE, así como diversos estados, han impulsado regulaciones y políticas orientadas a la protección de datos personales, considerándose activos de naturaleza

---

[208] "Independientemente de que se conciba el acceso a Internet como un derecho humano o fundamental, lo cierto es que hay un reconocimiento generalizado de que el acceso a Internet es indispensable para ejercer y disfrutar, de manera más plena, múltiples derechos humanos". Véase en Cecilia Serpa, "Escritura y Derecho: la narración de hechos desde una perspectiva sistémico-funcional", *Revista de la Facultad de Derecho de México* 7, nº 28 (2023): 5, doi:10.22201/fder.24488933e.2023.285.85404.

[209] Miguel Ángel Presno Linera, *Derechos fundamentales e inteligencia artificial* (Madrid: Marcial Pons, 2022), 37-43.

[210] "Implica estar permanentemente conectados a través de diversos sistemas y entornos digitales, como las redes sociales (RRSS), móviles, videoconferencias, cámaras, mensajería instantánea, mails, videollamadas, y todos estos servicios en movilidad que acompañan, en gran medida, la vida de los individuos". Véase en Arnaldo Hernández Guerra, "La persona hiperconectada: reflexiones desde el desarrollo humano, enfoque centrado en la persona", *Revista Comunicación* 30, nº 2 (2021): 5, doi:10.18845/rc. v30i2-2021.6030.

sensible. La UE, en 2022 aprobó la Declaración Europea sobre los Derechos y Principios Digitales[211] y en 2023, la Cumbre Iberoamericana, celebrada en República Dominicana aprobó la Carta Iberoamericana de Principios y Derechos en Entornos Digitales.[212] Ambos instrumentos de carácter declarativo, son un punto de partida para un marco regulativo en la protección de los datos personales nivel internacional.

Según el Reglamento General de la Protección de Datos Personales de la UE, se puede definir a datos personales, como:

> Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona […].213

Los datos personales, según este reglamento son toda información que permite identificar, de forma directa o indirecta, a una persona física. Se reconoce además que la identidad no puede estar reducida a nombres o números, sino que se basa en dimensiones físicas, psicológicas y sociales. Los datos personales no se tratan de simples registros, sino que son activos que pueden ser utilizados para perfilar, predecir o manipular conductas. Su proteccion es fundamental, sobre todo en entornos digitales donde la exposición y el acceso a los mismos es constante e intangible.

En el entorno virtual se habla de datos e imágenes sintéticos, que la Agencia Española de Protección de Datos define como, "Datos generados artificialmente, a diferencia de los datos reales que se recopilan de la realidad. Un conjunto de datos no reales, que se etiquetará como datos sintéticos, debe preservar las características y propiedades de los datos reales para un caso de uso específico",[214] un ejemplo claro de este tipo de datos es los *deepfakes*, aunque constituyen contenido sintético conservan características reales.

Los *deepfakes* son realizados en base a los datos personales y a partir de los mismos se desarrollan las imágenes y datos sintéticos que "No deben incluir información

---

[211] Moisés Barrio Andrés, *Los Derechos Digitales y su Regulación en España, la Unión Europea e Iberoamérica* (Madrid: Colex, 2023): 80-8.

[212] Ibíd.,88-90.

[213] UE Parlamento y Consejo Europeo, *Reglamento General de Proteccion de Datos de la Unión Europea*, 27 de abril de 2016, art. 4 numeral 1, A/RES/2016/679.

[214] AEPD Agencia Española de Protección de Datos, "Datos sintéticos y protección de datos", párr. 2, accedido 23 de enero de 2026, https://www.aepd.es/prensa-y-comunicacion/blog/datos-sinteticos-y-proteccion-de-datos.

identificable; al conservar únicamente propiedades estadísticas de los datos reales para fines específicos, permiten su uso sin tratar directamente datos personales, protegiendo así la privacidad y evitando riesgos legales".[215] Estos datos constituyen un resguardo de los datos reales siempre que carezcan de información que permita identificar a la persona de alguna manera o pueda su información ser identificable.

Respecto a las imágenes artificiales, Jorge Franganillo sostiene lo siguiente:

> Antes se podía notar una sensación de extrañeza ante la mirada vacía de una persona artificial, lo que se conoce como «efecto del valle inquietante». Pero hoy las imágenes son tan convincentes que nos llevan más allá de ese valle, a un mundo donde el engaño es más sutil y donde las caras producidas por IA no solo se confunden con las reales, sino que además generan más confianza.[216]

La evolución de las imágenes creadas mediante IA evidencia que hemos dejado atrás el clásico "valle inquietante", en donde las imperfecciones generaban desconfianza. Actualmente, la sofisticación tecnológica produce rostros tan convincentes que no sólo se confunden con los reales, sino que incluso generan credibilidad. De esta manera los *deepfakes*, al constituir imitaciones altamente verosímiles de la realidad, representan un riesgo significativo cuando se emplean para manipular contextos reales.

La accesibilidad en la creación de *deepfakes* ha generado vulneraciones a derechos fundamentales como la intimidad; en este sentido, la Corte Constitucional ha reconocido este derecho como, "El derecho a la vida privada y familiar que exige una obligación de abstención por parte del Estado",[217] reconociéndolo como un espacio de libertad inviolable del individuo, en el cual la persona puede desarrollarse sin interferencias arbitrarias. En contraste, al derecho de intimidad surge la libertad de expresión, reconocida en el Pacto Internacional de Derechos Civiles y Políticos CIDH,[218] o la Declaración de Naciones Unidas (ONU).

El derecho a la libertad de expresión sirve "Para que cada persona pueda manifestarse de forma autónoma y para singularizarse respecto a los demás sujetos que integran la sociedad".[219] La libertad de expresar ideas propias de manera autónoma, se

---

[215] Ibíd., párr. 8.

[216] Jorge Franganillo, "La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos", *Methaodos revista de ciencias sociales* 11, nº 2 (2023): 9-12, doi:10.17502/mrcs. v11i2.710.

[217] Ecuador Corte Constitucional, "Sentencia", en *Juicio n.º: 11-18-CN/19*, 19 de junio de 2019, párr. 176.

[218] ONU Asamblea General, *Pacto Internacional de Derechos Civiles y Políticos*, 16 de diciembre de 1966, art. 19, A/RES/21/2200 A.

[219] Presno Linera, *Derechos fundamentales e inteligencia artificial*, 53-60.

vincula a la resistencia y su alcance con las nuevas tecnologías puede traspasar líneas divisorias, exige responsabilidad con los derechos de los demás. Este derecho es esencial en el orden democrático, pero también la protección de la intimidad.[220] En caso de conflicto, será el juez constitucional quien decidirá el derecho que deberá prevalecer.

El derecho a la intimidad se relaciona con el derecho a la privacidad, ambos protegen la dignidad del ser humano, en contexto digitales se puede precisar la privacidad, como "[…] el derecho humano fundamental de la personalidad consistente en la facultad que tienen los individuos para no ser interferidos o molestados por persona o entidad alguna".[221] El derecho a la privacidad entendido como el resguardo de la esfera intima de la persona, se ve vulnerado con la creación y exposición de imágenes falsas de carácter sexual.

Al ser su protección prioritaria, se ha desplegado garantías normativas y jurisdiccionales para proteger y tutelar estos derechos frente a posibles vulneraciones. La CRE de 2008, no contemplaba un marco regulatorio para estas nuevas amenazas, derivadas de tecnologías digitales. Sin embargo, las garantías jurisdiccionales y especialmente la acción de habeas data,[222] positivizada en la norma constitucional constituyen una posible solución, para precautelar los derechos que se ven comprometidos por las nuevas creaciones digitales.

2.1. Habeas data: protección de datos personales en el entorno digital

Las nuevas creaciones digitales, exigen una revisión normativa evaluando la eficacia de protección de los datos y la capacidad de enfrentar la proliferación de contenido manipulado como *deepfakes* pornográficos. En la sentencia Nº 2064-14-EP/21,[223] la Corte, ha establecido la protección de los datos personales como un derecho fundamental, de aplicación directa, exigible a través de la acción de habeas data. Siendo una garantía jurisdiccional,[224] reconocida en la CRE y en la Ley Orgánica de Garantías

---

[220] Alonso Gómez Robledo Verduzco, *El derecho a la intimidad y el derecho a la libertad de expresión: Derechos humanos fundamentales* (San José: Corte Interamericana de Derechos Humanos, 2015), 15, https://biblioteca.corteidh.or.cr/tablas/aa12015.pdf.

[221] Ernesto Villanueva, *El derecho de la información* (México, Instituto de Investigaciones Jurídicas de la UNAM, 2003), 7, citado en Angie Dayana Ponce Cedeño, Génesis Karolina Robles Zambrano, y Ingrid Joselyne Díaz Basurto, "La inteligencia artificial y el derecho a la intimidad-privacidad", *IUSTITIA SOCIALIS* 8, n.˚ 1 (2023): 4, doi:10.35381/racji. v8i1.2493.

[222] Ecuador, *Constitución de la República del Ecuador*, art. 86.

[223] Ecuador Corte Constitucional, "Sentencia", en *Juicio n.º: 2064-14-EP*/21, 27 de enero de 2021, 17-25.

[224] Ecuador, *Constitución de la República del Ecuador*, art.92.

Jurisdiccionales y Control Constitucional,[225] como una herramienta de tutela frente a posibles vulneraciones.

El significado, de habeas data como señala el autor Martín Eduardo Pérez, proviene de dos voces latinas "Hábeas, viene de habere, que significa tener en posesión, y data, que proviene de datum, que significa hechos o instrucciones de forma apropiada para la comunicación por medios automáticos".[226] La definición se deriva del habeas corpus cuyo significado es que tengas el cuerpo; en el caso del habeas data es que tengas los datos. Su objetivo consiste en proteger los datos íntimos de los ciudadanos y evitar cualquier tipo de vulneración que se cause el uso indebido de los mismos.

Respecto a la protección de datos, las distintas legislaciones observan la convergencia de principios comunes como el consentimiento informado, la confidencialidad y el acceso a la información personal.[227] Se trata de principios básicos en la proteccion de datos, cuya divulgación está prohibida, salvo mediante autorización judicial. En consecuencia, quien elaboran y difunde *deepfakes* pornográficos, al recopilar datos personales de las víctimas como fotografías, nombres u otra información, sin su consentimiento vulneran directamente el derecho a la protección de datos personales.

La información personal como, por ejemplo "El origen racial o étnico, las opiniones políticas, las convicciones filosóficas o religiosas, la pertenencia a sindicatos, así como la referida a la salud o la sexualidad, han sido consideradas como información sensible".[228] Se trata de datos alojados en plataformas digitales que, en apariencia, resultan intrascendentes o neutros. Sin embargo, basta un cambio de contexto o de propósito para que se transformen en instrumentos de vulneración. Cuando esto ocurre es la persona quien ve comprometidos sus derechos esenciales y su dignidad.

Para dimensionar el alcance del daño, que puede llegar a tener el mal uso de los datos sensibles, puede citarse el siguiente ejemplo:

---

[225] Ecuador, *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*, Registro Oficial 52, Suplemento, 22 de octubre de 2009, art. 15.

[226] Martín Eduardo Pérez Cázares, "El habeas data o derecho a la intimidad en el derecho informático", *Revista del Instituto de Investigaciones Legislativas del Congreso del Estado de México* 15, n.° 98 (2021): 2, https://www.ordenjuridico.gob.mx/Congreso/pdf/98.pdf.

[227] "El derecho a la proteccion de datos personales o autodeterminación de la información tiene sus orígenes en 1970, cuando países europeos empiezan a dictar leyes que regulan la protección de datos personales, pero con el objetivo de regular las tecnologías [...]". Véase en Claudia Orellana Robalino, "De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales.", *FORO Revista de Derecho*, n. º 27 (2017): 7, https://revistas.uasb.edu.ec/index.php/foro/article/view/498/485.

[228] Mariliana Rico Carrillo, *Derecho de las nuevas tecnologías* (Buenos Aires: Ediciones La Roca, 2007): 166-70.

> Un caso doloroso de la historia nos ha enseñado que la amalgama compuesta por el uso de la tecnología y el tratamiento indebido de datos personales contribuyó al exterminio de más de seis millones de personas […] IBM mediante sus máquinas para tarjetas perforadas dotó al III Reich de capacidad para identificar a judíos, homosexuales, gitanos, izquierdistas y no arios, para confiscar sus propiedades, desplazarlos hacia los ghettos y campos de concentración y finalmente exterminarlos.[229]

La empresa tecnológica IBM, reconocida por sus aportes a la informática, desarrolló la máquina Hollerith, diseñada para procesar tarjetas perforadas con datos personales. Esta tecnología fue utilizada en el censo alemán de 1933, permitiendo la clasificación de ciudadanos según criterios como nombre, dirección y genealogía. Bajo el régimen nazi, esta capacidad de perfilación facilitó la identificación sistemática de personas por motivos étnicos, nacionales y otros rasgos sensibles, contribuyendo a una de las más atroces vulneraciones de derechos fundamentales en la historia contemporánea.

Desde el inicio de internet y las nuevas tecnologías, el manejo de datos a través de la web tiene una reconfiguración, "El uso creciente de las bases de datos para acceder información sobre las personas hace que las mismas sean, a la luz de los lectores de dicha información, lo que reflejen sus datos personales o lo que se interprete de los mismos".[230] La interpretación de los datos íntimos es subjetiva, porque lo que para una persona es privado para otra puede no serlo. Aun así, los daños derivados de su uso indebido son imprevisibles, lo que hace esencial fortalecer su esfera de protección.

La autora Simona Fanni menciona que las bases de datos cuando contienen información privada deben ser protegidas en la esfera digital, su criterio es el siguiente:

> En concreto, la *privacy* se reconoce como un derecho esencial para la protección de la dignidad humana y de la autonomía humana, que tiene que ser protegido durante todo el ciclo de vida de los sistemas de IA, tanto a nivel individual como a nivel colectivo. Por lo tanto, es crucial que los datos se recolecten, compartan y archiven de manera conforme a los valores y a los principios contemplados en la *Draft Recommendation*.[231]

Privacy, es un anglicanismo que se refiere el derecho a la intimidad, su protección es importante en la esfera digital debido a que abarca el uso de datos personales frente a los algoritmos de IA, que pudiesen vulnerar derechos a nivel personal y colectivo, tomando en cuenta la información de entrenamiento o *baby data*, que los desarrolladores han incorporado en plataformas digitales. El *Draft Recommendation*, refiere a una

---

[229] Ibíd., 167-75.

[230] Mariliana Rico Carrillo, *Derecho de las nuevas tecnologías*, 176-80.

[231] Simona Fanni, "La inteligencia artificial y el cuerpo humano digital: a la búsqueda del habeas data.", *IUS ET SCIENTIA* 6, n.° 2 (2020): 180, doi:10.12795/IETSCIENTIA. 2020.i02.13.

recomendación emitida por la UNESCO, que establece principios como el respeto a la dignidad y la protección de datos personales.

El habeas data ha evolucionado, con la inmersión de la IA y las nuevas creaciones digitales, es concebido como:

> Un componente esencial de los derechos fundamentales, especialmente en un mundo donde la información personal se ha convertido en un recurso valioso y, a menudo, explotado. […] la evolución del Habeas Data refleja no solo el reconocimiento de la importancia de la privacidad y la protección de datos, sino también un compromiso con la dignidad humana en un contexto global en constante cambio.[232]

En una sociedad moderna, el habeas data se vincula con la protección de datos en plataformas digitales. La vulneración de derechos personales a través de estos datos no es un riesgo hipotético, sino una realidad. En la práctica todas las personas se encuentran expuestas, incluso si los datos han sido recolectados con fines lícitos. El problema surge cuando dicha información, es utilizada con fines diversos a los previamente autorizados. El habeas data, ya normativizado debe adaptarse a esta nueva realidad tecnológica, ampliando su alcance y capacidad de respuesta.

El habeas data, trata de "Garantizar accesar y verificar la información, y como consecuencia pedir que se actualice los datos, rectificarlos o anularlos si fueren erróneos o afecten a derechos fundamentales como la honra o la intimidad".[233] Por tanto, se trata de una proteccion jurídica inmediata para hacer frente a las nuevas creaciones artificiales, impidiendo que la situación de la persona se agrave al difundirse de manera masiva en las redes sociales, en la que no sólo se altera el contenido original, sino que además pierde el control de sus datos personales.

De esta manera, las nuevas tecnologías como las creaciones audiovisuales de carácter artificial, presentan beneficios evidentes, pero también generan desafíos en el ámbito social. Ante este escenario las instituciones jurídicas deben evolucionar al ritmo de la sociedad. El habeas data, aunque es una figura tradicional en el derecho constitucional, su alcance puede perfectamente ayudar a enfrentar los desafíos que plantea la nueva era de la IA. El abogado y especialista en derecho constitucional, Cristian Masapanta, señala:

---

[232] Odette Martínez Pérez, Edward Fabricio Freire Gaibor, y Luis Alberto Alzate Peralta, "Desafíos del habeas data en la protección de datos personales en el ordenamiento jurídico ecuatoriano", *European Public & Social Innovation Review* 2, n.° 9 (2024): 3, doi:10.31637/epsir-2024-1842.

[233] Juan José Páez Rivadeneira y Santiago Acurio del Pino, *Derecho y Nuevas Tecnologías* (Quito: Corporación de Estudios y Publicaciones CEP, 2010): 145-50.

> […] cuando se genera una norma constitucional, el constituyente no podría haber predicho las nuevas situaciones en torno a las nuevas tecnologías, por más que se hubiese proyectado a futuro y no podemos convocar nuevamente a los constituyentes de Montecristi para añadir una "capítulo especial" a la Constitución. Pero sí podemos impulsar desarrollos jurisprudenciales desde órganos constituidos, como la Corte Constitucional del Ecuador, que actúa como intérprete supremo de la norma fundamental. Un ejemplo de esta adaptación se refleja en la sentencia 2064-14-EP/21, donde la Corte reconoció que la publicación no consentida de imágenes íntimas vulnera derechos conexos como la intimidad y la honra.[234]

La CRE en su art. 92, consagra la garantía del habeas data reconociendo el derecho de toda persona a acceder, actualizar y suprimir datos personales. Sin embargo, esta protección resulta insuficiente frente a los desafíos actuales, donde la tecnología afecta la dignidad e intimidad humana, de formas no previstas por el texto constitucional. Ante esta situación, el constitucionalista ecuatoriano Cristian Masapanta propone que sea la Corte Constitucional, a través de sus sentencias vinculantes, quien interprete y amplíe el alcance de esta garantía.

La sentencia 2064-14-EP/21, emitida por la Corte Constitucional es un precedente importante, marca una forma diferente de concebir los datos personales en el espacio digital. Además, de redefinir el alcance de esta garantía y reconocer la autodeterminación informativa, el derecho al olvido y la intimidad como dimensiones vulnerables ante las nuevas tecnologías; en este fallo la Corte ordena medidas de reparación y proteccion frente a la exposición digital.

El autor Néstor Sagues, señala que según la acción que se pretenda ejercer, en la doctrina esta garantía puede clasificarse en diferentes tipos:

> Una clasificación de los diversos tipos de habeas data: a) habeas data informativo: cuando se utilice para obtener la información nominativa determinada […] ; b) habeas data aditivo, aquel que trata de actualizar o incluir datos o información dentro de los archivos, […] c) habeas data rectificador o correctivo cuyo objetivo es corregir informaciones falsas, inexactas o imprecisas […] d) habeas data reservado, tiene por objeto asegurar que un dato determinado sea proporcionado a quienes se encuentran legalmente autorizados para conocerlo; e) habeas exclutorio o cancelatorio: se trata de eliminar información almacenada en algún banco de datos o sistema de información.[235]

El habeas data y su clasificación adquiere relevancia frente a los *deepfakes* pornográficos, que se crean a partir de datos personales obtenidos sin consentimiento. En el caso del habeas data informativo permitiría identificar la información que ha sido

[234] Cristian Masapanta, entrevistado por la autora, 15 de agosto de 2025. Para leer la entrevista completa, ver Anexo 5.

[235] Marcía Muñoz del Alba Medrano, *Habeas Data* (Ciudad de México: Instituto de Investigaciones Jurídicas UNAM, 2006): 5-15.

utilizada, el rectificador servirá para corregir distorsiones que afectan la identidad de la víctima. Asimismo, el habeas data reservado, limitaría el acceso a datos sensibles solo a quienes estén legalmente autorizados; y en el cancelatorio, se podría solicitar la eliminación definitiva de registros que perpetúan la vulneración.

En base a la sentencia N.º 2064-14-EP/21,[236] emitida por la Corte Constitucional, la misma aborda el caso del tratamiento no consentido de datos personales, específicamente fotografías intimas que fueron almacenadas y difundidas sin autorización. Ante esta situación, se mencionó lo siguiente:

> Se puede colegir que la fotografía de una persona constituye efectivamente un dato personal, ya sea porque identifica al individuo o porque lo hace identificable. La imagen puede revelar la identidad de la persona (es decir que la identifica), por ejemplo, cuando contenga su rostro, aunque también podría ser que cuente con algún otro elemento que inmediatamente permita reconocer la identidad del titular de ese dato, tal como su número de cédula, identificación o nombre. A su vez, también se constituye en dato personal aquella fotografía que, si bien no contiene el rostro de esta o algún otro elemento que la identifique de manera inmediata, permitiría el reconocimiento de aquella de manera mediata (es decir que la hace identificable).[237]

La Corte, ha reconocido que la fotografía de una persona constituye un dato personal relevante en tanto permite su identificación directa o indirecta, y no depende exclusivamente de la visibilidad del rostro, sino también de otros elementos que pueden vincularse a la imagen como el nombre, número de identificación, entorno físico, tatuajes o características particulares, todos estos detalles hacen a la persona identificable. La sentencia emitida por la Corte muestra una visión progresista al ampliar el espectro de los datos personales e incluir la imagen en fotografías.

El caso se aproxima a lo ocurrido recientemente en Australia, donde se reconoció que todos los ciudadanos son titulares de su imagen digital y pueden defenderla frente a usos algorítmicos indebidos,[238] se trata de un caso pionero de *deepfakes* pornográficos que motivó sanciones y reformas, se anunció restricciones al acceso de herramientas de IA que alteren imágenes conforme a la propuesta de establecer niveles de riesgo, el Comité Selecto sobre IA de este país propuso exigir la remuneración justa por el uso de imágenes en el entrenamiento algorítmico.

La protección de datos personales, según señala la Corte, se trata de:

---

[236] Ecuador Corte Constitucional, en *Juicio n.º: 2064-14-EP/21*, 20.

[237] Ibíd.,27-30.

[238] CaseGuard, "Australia evalúa nuevas normas sobre reconocimiento facial", *AI Redaction & Privacy for All*, accedido 10 de octubre de 2025, párr. 5, https://caseguard.com/es/articles/australia-evalua-nuevas-normas-sobre-reconocimiento-facial/.

> Carácter personal es un derecho constitucional en sí mismo, cuya vigencia no depende de que confluyan otros derechos constitucionales como la intimidad, honra y buen nombre. Por lo tanto, este derecho es directamente exigible a través de la acción de hábeas data, sin que se deba verificar primero una vulneración a otro derecho constitucional como la intimidad, privacidad, honra y buen nombre en la sentencia se observa que, aunque la accionada ha si ha descargado las imágenes.[239]

Se tiende a vincular el derecho a la protección de datos personales con los derechos a la intimidad, la honra y el buen nombre. Sin embargo, la Corte ha esclarecido que la protección de datos es un derecho autónomo, aunque guarde una estrecha relación en ciertos escenarios, no es lo mismo. En el caso concreto objeto de la sentencia, se dio un tratamiento indebido de datos personales, lo cual vulneró este derecho. Ante tal situación, la persona afectada tenía la potestad de interponer el habeas data como mecanismo reparatorio por la afectación provocada a sus derechos.

La víctima puede solicitar medidas cautelares de carácter constitucional, se señala que, "Se podrán ordenar medidas cautelares conjunta o independientemente de las acciones constitucionales, con el objeto de evitar o hacer cesar la violación o amenaza de un derecho".[240] Estan diseñadas para cesar el daño cuando es inminente a un derecho constitucional, las mismas pueden ir acompañadas por acciones como el habeas data o solicitarse de manera autónoma. Ante la proliferación de imágenes sexuales no consentidas, se puede solicitar el retiro inmediato del contenido digital dañino.

El habeas data en casos de datos e imágenes sintéticas, sirve para proteger la intimidad y el consentimiento de las personas. Podría hablarse de tratamiento de datos, pues la creación de *deepfakes* implica almacenamiento y uso de información que debe someterse a principios de consentimiento y finalidad.[241] La jurisprudencia constitucional ya ha reconocido su alcance en situaciones de difusión no consentida de imágenes íntimas, pero la ley no regula si al ser creaciones artificiales existe la posibilidad de vinculación con una persona y al ser identificada se aplica la protección de datos o no.

En el caso europeo, el Reglamento General de Protección de Datos[242] no menciona de manera expresa los datos sintéticos ni las imágenes generadas artificialmente. Sin embargo, la doctrina especializada ha comenzado a debatir su alcance dentro del concepto de dato personal señalando que mientras conserven patrones que permitan la

---

[239] Ecuador Corte Constitucional, en *Juicio n.º: 2064-14-EP/21*, 53-55.

[240] Ecuador, *Constitución de la República del Ecuador*, art. 35.

[241] Consentimiento. - Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo […] Finalidad. - Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular. Ecuador, *Ley orgánica de protección de datos personales*, arts. 8 y 10 lit. d.

[242] Europa, *Reglamento General de Proteccion de Datos de la Unión Europea Nº 2016/ 679.*

identificación indirecta de personas reales, deben ser tratados como datos personales.[243] De esta manera, la protección jurídica se extendería a la reidentificación y se puede pensar en categorías intermedias que regulen los riesgos.

A continuación, se presenta un organizador respecto al habeas data:

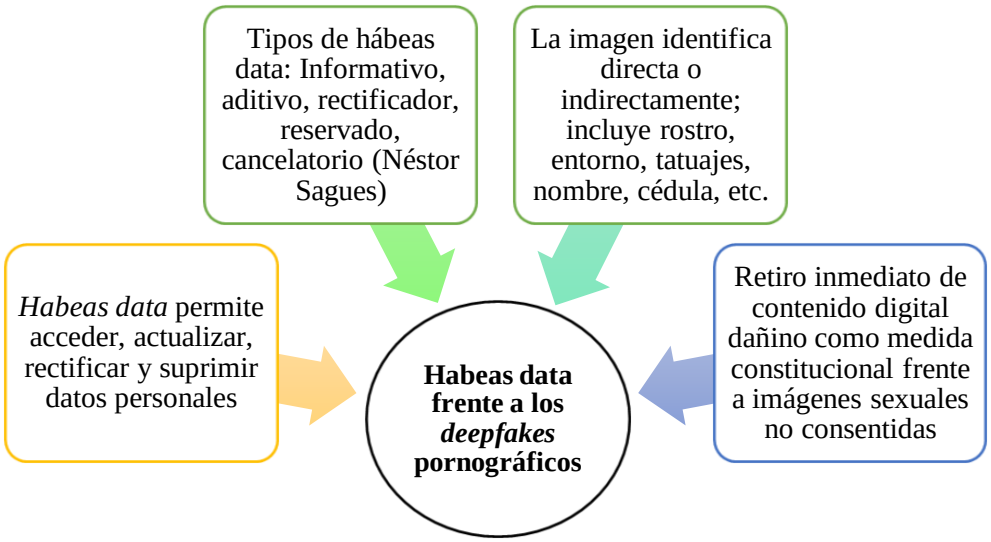


Figura 7. El habeas data como garantía constitucional, 2021
Fuente: Adaptado de la Sentencia Nº 2064-14-EP/21 de Corte Constitucional

3. Desafíos penales: ciberdelitos en el contexto de la inteligencia artificial

Al igual que la afectación de los derechos en la esfera constitucional ya no sólo se da a través del plano físico, con el aparecimiento de las nuevas tecnologías los delitos se configuran a través del entorno digital. Esta nueva modalidad delictiva, a criterio del autor Eloy Velasco Núñez, se puede definir como "Aquellos delitos que, en parte o en todo se desarrollan a través de las nuevas tecnologías, y que además de internet y la informática, pretenden agrupar bajo su denominación los que se producen a través o contra otras nuevas tecnologías como: el cloud computing, el tratamiento del big data, el internet de las cosas, el blockchain, la inteligencia artificial".[244]

El internet, constituye el punto de expansión de las nuevas tecnologías, así como han generado beneficios a la sociedad, también ha hecho posibles formas inéditas de vulneración. Las nuevas tecnologías incorporadas como *cloud computing*, el *big data* o *el internet de las cosas*, han facilitado el acceso y tratamiento ilícito de datos personales. En el ámbito financiero, la tecnología *blockchain*, ha sido utilizada para ocultar la

[243] Agencia Española de Protección de Datos, "Datos sintéticos y protección de datos", párr. 4.
[244] Eloy Velasco Núñez, *Delitos tecnológicos Cuestiones penales y procesales* (Madrid: Wolters Kluwer S.A., 2021), 23-30.

identidad o apropiarse de fondos de forma ilícita. Finalmente, la IA ha sido cuestionada debido al impacto que puede tener en los derechos de las personas.

Según Pablo Palazzi, "El estudio de delitos donde la informática juega un papel preponderante, ya sea porque se utiliza para medio para delinquir o porque es el objeto del delito en sí".[245] Se debe diferenciar dos modalidades de delitos, los delitos informáticos, que son "Toda aquella acción antijurídica dada por vías informáticas cuyo objeto es dañar ordenadores, medios electrónicos y redes de internet".[246] Su afectación se basa en el sistema informático, son una agresión técnica, como el ataque a sistemas informáticos, interceptación o revelación a bases de datos.

Por otro lado, los ciberdelitos son "Actividades ilícitas ejecutadas mediante tecnologías de la información y la comunicación (TIC), que atentan contra identidad, privacidad y seguridad de los datos personales".[247] Se trata de conductas lesivas orientas a afectar bienes jurídicos de las personas, cuyo medio de comisión se origina en el uso indebido de la tecnología. Ambas clases de delitos digitales constituyen ilícitos difíciles de investigar y juzgar, debido a su comisión en entornos virtuales que apenas dejan rastro.

A manera de antecedente en "EE. UU. comenzaron los casos de delitos informáticos surgiendo en parte relacionados con el secreto comercial". [248] En contextos en los que la información confidencial empezaba a representar, una ventaja competitiva en diseños de fórmulas, bases de datos y la vulneración de acuerdos de confidencialidad. Más adelante, estos delitos se perfeccionaron y diversificaron a diferentes áreas sociales, cuyos ordenamientos jurídicos tradicionales dificultaban su persecución y castigo por tanto nace la categoría de cibercrímenes.[249]

En la década de los 90´s, ente los primeros delitos digitales conocidos aparece *hacking,* en "1989 cuando una investigación criminal en Alemania detectó varios *hackers* que usaban redes internacionales para acceder a la información americana e inglesa y

[245] Palazzi, *Delitos Informáticos*, 26-28.

[246] Gustavo Andrés López Rincón y Laura Marcela Quintero Sánchez, "Delitos contra la intimidad personal en el marco de la inteligencia artificial en Colombia", *Postulados: Revista Socio Jurídica* 1, nº 2 (2025): 5, doi:10.22463/29816866.4300.

[247] Geovanna Gabriela Espinosa Carvajal y Fernando Eduardo Paredes Fuentes, "Los ciber delitos y la protección de datos personales en el sistema penal ecuatoriano", *Revista Lex* 8, nº 29 (2025): 4, doi:10.33996/revistalex. v9i28.302.

[248] Palazzi, *Delitos Informáticos*, 35.

[249] "[...] los denominados cibercrímenes permiten tutelar bienes jurídicos tradicionales como la vida privada; la honra y dignidad; la integridad y libertad sexual; el patrimonio; la seguridad jurídica; y la buena administración pública". Véase en Juan Pablo Albán Alencastro et al., *Regulación del Internet y derechos digitales en Ecuador* (Quito: Editorial USFQ, 2016): 32.

venderla a los servicios secretos de la KGB".[250] El caso se trata de una operación de ciber espionaje en donde un grupo de hackers alemanes accedió de forma ilícita a información confidencial del gobierno estadounidense e inglés, la cual fue posteriormente comercializada con los servicios de inteligencia soviéticos.

Más adelante, aparece "La denominada *piratería informática*, la manipulación de cajeros automáticos y el abuso de telecomunicaciones, que revelaron lo vulnerable que eran los sistemas".[251] A partir de ello, se entendió el delito informático de manera más amplia, pues ya no sólo afectaba a los datos sino a las personas titulares de dicha información. Esta evolución conceptual permitió incorporar dimensiones jurídicas que vinculan el daño informático con la afectación de bienes jurídicos, abriendo paso a nuevas categorías de protección en el ámbito penal.

En 2001 el Consejo de Europa emitió el Convenio de Budapest,[252] este instrumento incluye ciberdelitos relacionados con pornografía infantil, enunciando la prohibición difusión y posesión, de este tipo de contenido a través medios informáticos. Se trata del primer tratado internacional que aborda los delitos cibernéticos, en el caso de Ecuador en 2024 la Asamblea Nacional aprobó la adhesión a este Convenio, [253] se prevé que se establezca una política penal común para proteger a la sociedad frente a la ciberdelincuencia.

Posteriormente, se creó un Segundo Protocolo Adicional,[254] adoptado en 2022 y se espera que Ecuador también forme parte. Este Protocolo faculta a los estados, a requerir de los proveedores de internet la entrega de información como direcciones IP, cuando sea necesario para una investigación penal.[255] En el caso de los *deepfakes* pornográficos, serviría para determinar el origen del contenido, aunque se encuentre en otro país la dirección IP asociada a la cuenta que publica el contenido dañino, ayudando a preservar la evidencia digital y fortalecería la cooperación internacional entre países.

3.1. Bienes jurídicos afectados por los *deepfakes* pornográficos

La proliferación del contenido artificial de carácter pornográfico, constituye una forma de violencia digital que vulnera diversos bienes jurídicos. En el centro de esta

[250] Palazzi, *Delitos Informáticos*, 38.
[251] Ibíd., 39.
[252] Consejo de Europa, *Convenio de Budapest contra la Ciberdelincuencia*, art.6.
[253] Crespo, "Transformer", párr. 7.
[254] UE Consejo de Europa, *Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia*, 23 de noviembre de 2001, art. 1, A/RES/132/224.
[255] Ibíd., art. 7.1.

afectación se encuentra la dignidad humana, como eje central de los derechos fundamentales. Asimismo, se ha observado en los casos de estudio, que se encuentran comprometidos bienes jurídicos como la intimidad, la indemnidad, la integridad física y psíquica, el honor y buen nombre y la privacidad; inclusive pueden generar impactos de carácter patrimonial, social y psicológico para las víctimas.

En la regulación penal ecuatoriana esta figura como delito autónomo o parte de otro delito aún no se ha tipificado, sin embargo, diversos estudios abordan esta problemática, señalando que la tecnología *deepfake* "Ofrece un abanico de posibilidades creativas y profesionales, pero su potencial para ser mal utilizado plantea un desafío urgente, es crucial que se desarrollen soluciones tanto tecnológicas como legales para abordar este problema",[256] esta postura sostiene que los *deepfakes,* son una tecnología novedosa pero lasciva para la sociedad, por tanto debe regularse.

La referencia de la tipificación de esta conducta exige una revisión de la teoría del delito, particularmente de los dos sistemas clásicos, como son: el causalismo y el finalismo. Desde la perspectiva causalista, se propone: "La acción humana como el hito causal que desencadena un resultado".[257] Esta teoría se centra en atribuir la culpabilidad a una persona que realiza una acción cuya relación causal se ve reflejada en el resultado. Pero no se puede culpabilizar a una persona por crear *deepfakes,* ya que como se ha visto pueden tener diferentes usos.

En contraste la teoría finalista formulada por Hans Welzel, a mediados del siglo XX, introduce una concepción más profunda de la acción humana, entendida como:

> La culpabilidad consiste en determinar si el comportamiento típico y antijurídico es atribuible y reprochable al sujeto, porque en el momento de actuar era plenamente capaz de entender la ilicitud de dicho comportamiento (imputabilidad), actuó conociendo dicha ilicitud (conocimiento de la antijuricidad del hecho) ya que cabe la posibilidad de realizar la acción en legítima defensa, y el sistema legal le podía exigir que actuara de otro modo (exigibilidad).[258]

En este enfoque, la culpabilidad se determinada a partir de la existencia de un comportamiento antijurídico, que puede ser reprochado al sujeto. La teoría se centra en la antijuridicidad de la acción, contempla las causas de exclusión de la antijuridicidad

[256] Renata Correa Peña, "Delito de Deepfake y Pornografía Infantil Generada por IA en la Legislación Ecuatoriana" (tesis académica, Universidad Católica de Cuenca, 2024), 36, https://n9.cl/kt48a.

[257] UAC, "Teoría del delito. Evolución. Elementos Integrantes", *Universidad Andina del Cusco, Perú,* 15 de junio de 2018, núm. 29, https://ficp.es/wp-content/uploads/2019/03/Barrado-Castillo.-Comunicaci%C3%B3n.pdf.

[258] Ibíd., párr. 3.

como el estado de necesidad o legítima defensa, que permiten eximir determinadas conductas en contextos excepcionales. En el caso de los *deepfakes* pornográficos, el análisis revela que la acción está orientada a un fin lesivo y se trata de causar daño a la persona, ya sea este de carácter reputacional, patrimonial, social o familiar.

La teoría del delito desde el punto de vista de su aplicabilidad sugiere que "El delito en Ecuador enfrenta desafíos considerables en su aplicación, derivados de las complejidades de una sociedad en constante cambio, la influencia de factores sociales, económicos y tecnológicos plantea nuevos dilemas en la tipificación de conductas delictivas".[259] Las nuevas tecnologías proponen modalidades emergentes de daño en contra de los bienes jurídicos protegidos. La forma novedosa de cometer delitos exige un sistema flexible, que pueda ser aplicable a la nueva realidad social.

Mediante la adopción de nuevos tipos penales, relacionados con el cibercrimen se ha podido llegar a tutelar bienes jurídicos, como: la honra, la dignidad, la integridad, la libertad sexual, el patrimonio, la seguridad jurídica y la buena administración pública. En ese sentido, un bien jurídico se puede definir como, "Aquellos objetos que merecen protección jurídico penal".[260] Se trata de derechos considerados importantes para la persona, que son protegidos en la esfera penal. El propósito de su protección es evitar su vulneración, ya sea que se traten de bienes jurídicos nuevos o tradicionales.

Así se establece en el COIP, cuya promulgación en 2014 redefinió el marco penal ecuatoriano, esta normativa evidencia entre algunos delitos la pornografía infantil, la violación de la intimidad, el fraude cibernético, la falsificación cibernética, la interceptación ilegal de datos, el ataque a la integridad de sistemas informáticos, la obtención de información pública reservada y el acceso no consentido a sistemas informáticos. Todos estos delitos se tratan de conductas perpetradas a través de internet, que dañan o ponen en riesgo determinados bienes jurídicos.

Antonio Vinelli los denomina delitos pluriofensivos, porque "No solamente se salvaguarda el sistema de información, sino también otros bienes jurídicos "clásicos" como, por ejemplo, el patrimonio o la intimidad".[261] Estos delitos son denominados pluriofensivos, porque si bien nacen del mal uso de la tecnología su afectación se

[259] Gloria Rosana Urbina Carvajal et al., "Evolución y Aplicación de la Teoría del Delito en el Sistema Penal Ecuatoriano", *LexEnlace Revista Científica Jurídica* 1, nº 2 (2024): 9, https://lexenlace.com/wp-content/uploads/2024/12/LEX-AC77.pdf.

[260] Albán Alencastro et al., *Regulación del Internet y derechos digitales en Ecuador*, 32-35.

[261] Renzo Antonio Vinelli Vereau, "Los delitos informáticos y su relación con la criminalidad económica", *Ius et Praxis* 53, nº 1 (2021): 13-16, doi:10.26439/iusetpraxis2021.n053.4995.

diversifica a diferentes aspectos de la esfera personal e íntima. En el caso de los *deepfakes* pornográficos si bien su impacto vulnera múltiples bienes jurídicos, principalmente debería protegerse la dignidad humana como eje central.

Según la opinión del abogado y especialista en Derecho Penal Informático Santiago Acurio del Pino, menciona que:

> Los *deepfakes* pornográficos, que en este caso afectan, a la intimidad, a la privacidad, a la propia imagen de una persona, no es un delito de carácter sexual, sino es un delito contra la dignidad del ser humano. […] hay que tener en cuenta que en el tema de delitos informáticos o delitos cibernéticos en este caso son delitos pluriofensivos. Básicamente no es que tienes un bien jurídico protegido particular. Por eso entra justamente en el derecho a la propia imagen, el derecho a la intimidad, a la privacidad, a la propia protección de datos personales, debe protegerse la dignidad del ser humano.[262]

El experto señala que los delitos cibernéticos, pueden afectar múltiples bienes jurídicos. En el caso de contenidos digitales como los *deepfakes* pornográficos, su creación y difusión vulnera la intimidad, el honor y la integridad. Tratándose de niños, niñas y adolescentes, el bien jurídico afectado se trata de la indemnidad sexual, y además otros bienes jurídicos como la privacidad, la imagen etc. Pero todos estos bienes jurídicos, deben entenderse como expresiones de uno sólo en común que los engloba y es la dignidad humana, la cual de manera estratégica debe ser protegida.

Además, de ser pluriofensivos también se podría establecer un posible ilícito que afecta intereses colectivos y difusos, al respecto se menciona:

> Los intereses difusos enseñan o ponen de manifiesto aquellos nuevos intereses colectivos, nuevos intereses de la mayoría de la población, respecto de los cuales no son operativos o proyectables las tradicionales técnicas de tutela penal, puesto que su efectiva y racional protección penal precisa de un complejo entramado institucional de organización y control.[263]

Los ciberdelitos han impactado gravemente interés colectivos y difusos, al afectar a grupos numerosos de personas que comparte un nexo en común, como el uso de plataformas digitales o la pertenencia a comunidades vulnerables. Además, no existe un titular del bien jurídico comprometido al tratarse de intereses difusos, todos los integrantes del grupo son simultáneamente titulares. Estas circunstancias dificultan la

---

[262] Santiago Acurio del Pino, entrevistado por la autora, 18 de agosto de 2025. Para leer la entrevista completa, ver Anexo 6.

[263] Gabriela Prado y Mario Durán Migliardi, "Sobre la evolución de la protección penal de los bienes jurídicos supraindividuales. Precisiones y limitaciones previas para una propuesta de protección penal del orden público económico en Chile", *Revista de Derecho Universidad Católica del Norte* 24, nº 1 (2017): 9, doi: http://dx.doi.org/10.4067/S0718-97532017000100263.

proteccion penal, para entender de mejor manera este fenómeno, se expone un caso de racismo en las hinchadas de la FIFA a través del entorno digital.

El caso anteriormente mencionado, se basa en lo siguiente:

> La FIFA ha multado a seis federaciones nacionales, incluida la campeona defensora Argentina, por abusos racistas por parte de los aficionados en las eliminatorias del Mundial en junio. Las seis naciones acusadas de "discriminación y abuso racista" fueron Albania, Argentina, Chile, Colombia, Serbia y Bosnia-Herzegovina, según la lista de sanciones publicada por la FIFA de su comité disciplinario.[264]

Este caso ejemplifica la manera en que la violencia colectiva se traslada al plano digital y a consecuencia de ello se refleja la acción disciplinaria que tomo la FIFA contra de seis federaciones nacionales por actos de discriminación y abuso racista cometidos por sus hinchas. Las conductas sancionadas incluyeron cantos ofensivos, mensajes inapropiados y expresiones racistas tanto en estadios, como en redes sociales. La violencia de las hinchadas se asemeja a la violencia digital ejercida a través de la divulgación de los *deepfakes* pornográficos, que afecta intereses colectivos y difusos.

En relación a la afectación de los derechos de los niños, niñas o adolescentes en el art.103 del COIP, se tipifica el delito de pornografía con la utilización de niños, niñas y adolescente, de la siguiente manera:

> Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años.[265]

Este tipo penal protege bienes jurídicos, como la libertad e integridad sexual además el desarrollo pleno de la personalidad del niño, niña o adolescente con particular énfasis la indemnidad sexual. La forma de comisión se configura al producir, filmar o grabar imágenes reales o simuladas de desnudos de menores de edad, exige una participación directa de la víctima ya sea través de contacto físico o registro visual. La pena impuesta se considera proporcional a la gravedad de la infracción y la prueba se suele sustentar en evidencia física que permite acreditar la materialidad del hecho.

---

[264] Graham Dunbar, "FIFA multa a Argentina y otras selecciones por racismo de hinchas en eliminatorias", *Independent en español*, accedido 9 de septiembre de 2025, párr. 1 y 2, https://www.independentespanol.com/deportes/fifa-multa-a-argentina-y-otras-selecciones-por-racismo-de-hinchas-en-eliminatorias-b2819526.

[265] Ecuador, *Código Orgánico Integral Penal COIP*, art. 103.

En los *deepfakes* pornográficos, al contrario del delito de pornografía infantil la participación de la víctima no exige el contacto físico, pero si la simulación visual. Se tratan de imágenes sintéticas generadas a través de GANs provenientes de IA generativa, cuya intención del autor se basa en incluir burlas, daño reputacional e inclusive acoso. Además de la indemnidad, también se denota otros bienes jurídicos afectados como la intimidad, la honra, la privacidad. Finalmente, para probarse la comisión de este delito se requiere peritaje digital[266] y análisis de simulación.

El delito de violación contra la intimidad, tipificado en el art. 178 del COIP, establece lo siguiente:

> Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.[267]

En la formulación del tipo penal se sanciona el acceso o divulgación de datos reales sin la debida autorización, en cuanto a la naturaleza del contenido se trata de información auténtica y jurídicamente protegida. La víctima ostenta la titularidad legítima de los datos vulnerados, cuya afectación se produce mediante medios digitales, sin que ello implique manipulación o alteración del contenido. Este delito se encuentra tipificado en el COIP y su acreditación probatoria se sustenta a través de la evidencia física y en la constatación del acceso no autorizado.

La creacion y difusión de *deepfakes* pornográficos, presenta un carácter de pluriofensivo, al vulnerar la dignidad humana y otros derechos conexos, mediante la simulación digital de contenido sexual sin consentimiento, utilizando tecnologías avanzadas como la IA, para alterar la imagen, la voz y el vídeo. Esta conducta se podría abordar como una forma de violencia digital; sin embargo, su complejidad técnica y su naturaleza sintética plantea la cuestión de si se debería incorporar en el mismo tipo penal o amerita la creación de una figura penal autónoma.

---

[266] "El software de detección de deepfakes se está volviendo cada vez más popular para proteger contra los efectos dañinos de videos y audios falsos, donde se estima que el mercado mundial de software de detección de deepfake exhibirá una tasa compuesta anual del 38,3% entre 2024 y 2029". Véase en Mario Micucci, "Herramientas para detectar deepfakes y combatir la desinformación", *welivesecurity*, accedido 11 de octubre de 2025, párr. 4, https://www.welivesecurity.com/es/seguridad-digital/herramientas-para-detectar-deepfakes-combatir-desinformacion/.

[267] Ecuador, *Código Orgánico Integral Penal COIP*, art. 178.

El especialista Acurio del Pino, propone tipificar la conducta de pornografía sintética, de la siguiente manera:

> La inteligencia artificial, como tecnología disruptiva, debe ser regulada sin temor, pues el miedo obstaculiza la innovación. Existe una tendencia internacional a equiparar los *deepfakes* sintéticos con la pornografía infantil real, lo que exige que Ecuador proteja los bienes jurídicos conforme al artículo 393 de la Constitución, garantizando la seguridad humana, incluida la cibernética. Esto se relaciona con el ius puniendi del Estado, sustentado en la teoría del contrato social de Rousseau. Se propone que esta conducta se subsuma al artículo 103 del COIP o se tipifique como delito autónomo, en armonía con el Convenio de Cibercrimen, que Ecuador ha ratificado y que otorga cinco años para adaptar la normativa y adherirse a sus protocolos.[268]

El autor propone una reforma para tipificar los *deepfakes* pornográficos como un delito autónomo, aunque también considera incorporar un agregado al artículo 103, siguiendo la recomendación del Consejo de Europa y el art. 9.2 del Convenio. De estas dos opciones, agregar un inciso al art. 103 sería más factible, tipificando y sancionando la pornografía sintética, dado que concebir un nuevo tipo penal es más complejo porque requiere demostrar la gravedad de la conducta mediante estudios criminológicos, definir el bien jurídico afectado, respetar el principio de mínima intervención penal y armonizar la norma con tratados internacionales, siendo la opción más recomendable al ser su configuración mejor estructurada.

Al considerar la nueva tipificación de delitos Helena Hernández, menciona:

> La historicidad y transformaciones sociales que atraviesa al derecho penal deben reflejarse en cambios de paradigmas y actualización en la tipificación de delitos, así como la nueva comprensión de bienes jurídicos. La IA generativa no siempre es empleada para buenos propósitos, realidad a la que debe responder cada legislación. Los *deepfakes* sexuales son una nueva forma de violencia sexual.[269]

El desafío de armonizar la modernidad tecnológica con las garantías penales, es el nuevo reto de la justicia penal; en tanto, que las transformaciones sociales impactan al derecho de manera similar sucede con el derecho penal. El mismo debe cambiar y adaptarse a las nuevas modalidades de delitos que aparecen con el avance de la tecnología y la IA. Las nuevas conductas exigen nuevas técnicas de proteccion de los bienes jurídicos y de investigación, para lograr una interceptación eficaz de quienes se encuentran tras el cometimiento de dichos delitos.

---

[268] Santiago Acurio del Pino, entrevistado por la autora, 18 de agosto de 2025. Para leer la entrevista completa, ver Anexo 6.

[269] Helena Hernández, "Los 'deepfakes' y el derecho penal", *Ámbito Jurídico*, accedido 10 de septiembre de 2025, párr. 13, https://www.ambitojuridico.com/noticias/columnista-impreso/constitucional-y-derechos-humanos/los-deepfakes-y-el-derecho-penal.

El anonimato favorece la impunidad en los cibercrímenes, Juan Albán et al., entiende como "[L]a percepción de seguridad con la que actúa el delincuente, ese temor mínimo a ser detectado o detenido, sin terceros que presencien el hecho, adoptando diversos nombres y personalidades falsas".[270] En sentido estricto no se puede hablar de anonimato a causa de la dirección IP o la huella digital, que genera un usuario al navegar en la red. En la práctica es difícil llegar a conocer la persona que se encuentra elaborando las posibles vulneraciones cibernéticas.

Los bienes jurídicos que busca precautelar la tipificación de nuevas modalidades delictivas corresponden a categorías previstas en el ciberespacio, entendido como "[E]l espacio virtual (no físico) de interrelación humana".[271] Haciendo referencia a una realidad digital que coexiste con la física, pero cuya trascendencia se proyecta sobre la misma, como ocurre con la creación de contenido pornográfico no consentido. Aunque dicha elaboración se produce en entornos virtuales, sus repercusiones afectan la vida de la persona generando impactos de los derechos en el mundo físico.

En la siguiente figura, se sistematiza los bienes jurídicos afectados a través de las dos infracciones penales tipificadas en los arts. 103 y 178 del COIP, así como una conducta susceptible de tipificación penal, como lo es la pornografía sintética.

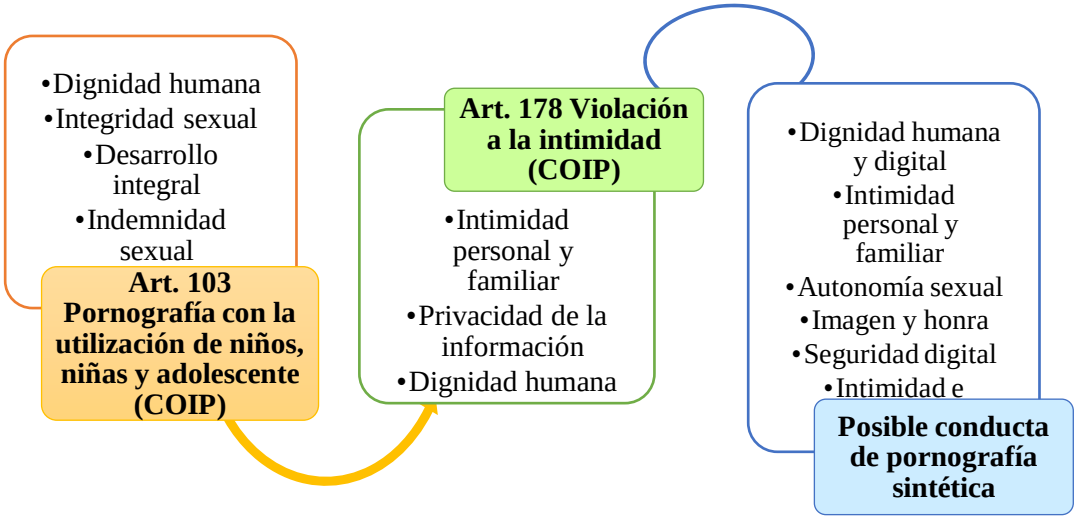


Figura 8. Delitos tradicionales y conducta de pornografía sintética en el entorno digital, 2025
Fuente: COIP, Albán Alencastro et.al.[272] , Eugenio Zaffaroni[273] y Santiago Acurio del Pino[274]

[270] Albán Alencastro et al., *Regulación del Internet y derechos digitales en Ecuador*, 49-52.
[271] Ibíd., 32-35.
[272] Ibíd., 35–60.
[273] Eugenio Raúl Zaffaroni, *La palabra de los muertos: conferencias de criminología cautelar* (Quito: Editorial El Siglo, 2018), 85–115.
[274] Páez Rivadeneira y Acurio del Pino, *Derecho y Nuevas Tecnologías*, 110–25.

En los casos de estudio, el delito investigado resultó insuficiente al no contemplar la generación de contenido pornográfico mediante IA, lo que plantea la necesidad de un nuevo tipo penal. Asimismo, aunque en la Constitucion, así como en el art. 77 núm. 11 del COIP, se reconoce a las víctimas el derecho a la reparación integral. En el proceso penal se requiere una sentencia condenatoria en firme y al haberse archivado la investigación, ninguno de los casos avanzó de la fase inicial, impidiendo acceder a la justicia y por tanto concretar la reparación integral.

3.2. Futura regulación de los *deepfakes* pornográficos en el entorno digital

El análisis de la legislación vigente revela la necesidad urgente de actualizar normas y prácticas administrativas para responder a los nuevos paradigmas contemporáneos. El derecho, como construcción social, debe evolucionar junto a la realidad, pues cuando la normativa no refleja las dinámicas actuales, se torna obsoleta e insuficiente para garantizar los derechos en un Estado constitucional fundado en la justicia social y la dignidad humana. En esta transición hacia la era artificial, los derechos fundamentales deben resguardarse en base al eje del desarrollo ético y normativo.

De esta manera, "Si la tecnología tiene una enorme capacidad de innovación, no la tienen menos los derechos fundamentales".[275] Las nuevas tecnologías ofrecen una oportunidad para fortalecer los derechos, mediante el reconocimiento y creación de mecanismos de protección ante su uso indebido. La formulación de nuevas regulaciones debe considerar algunos aspectos importantes, como la diferencia del avance tecnológico observado en Europa y Estados Unidos frente a América Latina, que aún enfrenta desafíos estructurales significativos en materia de inclusión digital.

Según la UNESCO en 2017, "Más de 200 millones de latinoamericanos permanecen desconectados, especialmente en zonas rurales".[276] Esta cifra revela que millones de latinoamericanos permanecen al margen de la revolución digital, como es de preverse la brecha no es solo técnica, sino también social, económica y educativa. Ante esta realidad, las posibles soluciones deben responder a la realidad social, regulando los

[275] José Ignacio Solar Cayón y Olga Sánchez Martínez, *El impacto de la inteligencia artificial en la teoría y la práctica jurídica* (Madrid: Wolters Kluwer Legal & Regulatory, 2022): 118–25.

[276] Hernán Galperin, *Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe* (París: UNESCO Programa MOST, 2017): 5-10, https://blogs.ugto.mx/mdued/wp-content/uploads/sites/66/2022/12/Sociedad-digital-brechas-y-retos-para-la-inclusion-digital-en-America-Latina-y-el-Caribe.pdf.

contenidos dañinos elaborados a través IA para prevenir la violencia digital, sin restringir el acceso a la tecnología.

En el contexto latinoamericano, se requiere implementar principios como, "La transparencia, accesibilidad, auditabilidad, explicabilidad, trazabilidad, fiabilidad, a la no discriminación algorítmica, a no ser objetivo de decisiones automatizadas, supervisión humana".[277] Pues como ya se ha visto, estas nuevas tecnologías pueden vulnerar derechos al reproducir sesgos y excluir subjetividades, incluso sin intervención humana. La futura regulación deberá ser flexible a la innovación, sin perder de vista el objetivo principal que es precautelar los derechos fundamentales.

Desde esta perspectiva, resulta relevante la opinión del abogado y eurodiputado Ibán García del Blanco, quien desempeñó un papel activo en la formulación de la Ley de IA de la Unión Europea, al señalar lo siguiente:

> La inteligencia artificial, entendida como producto, requiere una norma específica debido a sus circunstancias especiales, su potencia y su capacidad de generar daño, para ello se establecen categorías de riesgo. En cuanto a la inteligencia artificial generativa, la Ley incorpora un capítulo adicional de prevención centrado en normas de transparencia, exigiendo que los contenidos generados sean etiquetados como creados con IA. Además, si el uso de IA generativa afecta derechos fundamentales, deben aplicarse también normas sobre riesgos, incluyendo usos prohibidos o de alto riesgo. Finalmente, esto no implica que el resto del derecho pierda vigencia: la IA es tratada como una herramienta distinta, pero el derecho debe ser indiferente al medio utilizado sea IA o no.[278]

El entrevistado advierte sobre el carácter singular de esta nueva tecnología, lo que justifica la necesidad de normas específicas que contemplen sus riesgos inherentes. Además, menciona que, en base a la inteligencia artificial generativa y las creaciones digitales, en la normativa europea se ha pedido el etiquetado obligatorio es decir señalar que el contenido ha sido generado a través de IA. Aclara que indistintamente de la herramienta utilizada, debe normarse y sancionarse las vulneraciones en contra de los derechos fundamentales realizados a través de la tecnología.

En relación a detección y retiro de contenidos ilícitos, existe el Digital Services Act (DSA)[279], se trata de un reglamento vigente en la Unión Europea desde febrero de 2024, que establece un marco normativo para la notificación y retiro de contenidos ilícitos en plataformas digitales, exigiendo mecanismos accesibles y protección de derechos

---

[277] Ibíd., 119.

[278] Ibán García del Blanco, entrevistado por la autora, 20 de agosto de 2025. Para leer la entrevista completa, ver Anexo 7.

[279] UE Parlamento y Consejo Europeo, *Digital Services Act [DSA]*, 19 de octubre de 2022, art. 1, A/RES/2022/2065.

fundamentales. En Ecuador, su adaptación permitiría fortalecer la trazabilidad algorítmica y proteger la imagen digital como dato sensible, especialmente en casos que comprometen la dignidad de personas vulnerables.

El tema de la flexibilidad frente a los nuevos derechos, se analiza el art. 11 núms.3 y 8 de la CRE, que determina:

> El ejercicio de los derechos se regirá por los siguientes principios: […] Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. […] El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio.[280]

Mediante esta norma constitucional las víctimas de *deepfakes* pornográficos, no necesitan esperar una ley específica para exigir protección, se puede invocar directamente derechos constitucionales como la dignidad, la intimidad y la no discriminación ante cualquier autoridad pública, permitiendo ejercer la acción frente al daño. De manera que, si la sociedad evoluciona el derecho a través del principio de progresividad permite enfrentar las nuevas formas de vulneración tecnológica, sin que se encuentre normado para garantizar su protección.

Respecto a los nuevos proyectos de regulación de la IA en Ecuador, el entrevistado, señala:

> El mundo debería aprovechar la experiencia europea como pioneros en regulación, para establecer marcos normativos propios. Estos deben adaptarse a cada país, sin ser una copia, pero el espíritu de la norma sí debería ser escalable. […] creo profundamente que lo ideal es que hubiera cierta integración entre el área regional, es decir, porque al final estamos hablando de una materia que es muy compleja, que puede generar muchas dificultades, incluso porque los grandes desarrolladores de estas tecnologías, conocidos a nivel internacional, son muy poderosos. Es muy difícil competir, negociar o normar su actividad regulatoriamente, porque tienen mucha capacidad de influencia y presión.[281]

Podría considerarse como punto de partida la normativa vigente de la UE, pero no se trata de replicarla, sino de identificar el espíritu y los valores que la sustentan, especialmente en lo relativo a sanciones y clasificación de los riesgos derivados. Además, se menciona un desafío crucial, la creciente generalización de la IA, se propone una regulación articulada como bloque regional cuya idea no resulta ajena a la realidad, sino

[280] Ecuador, *Constitución de la República del Ecuador*, arts. 3 y 8.

[281] Ibán García del Blanco, entrevistado por la autora, 20 de agosto de 2025. Para leer la entrevista completa, ver Anexo 6.

que se perfila como una estrategia necesaria para enfrentar usos indebidos de IA que de otra manera no se podrían sancionar.

El jurista brasileño Antonio Wolkmer, frente al avance de la globalización, menciona que,

> Las nuevas formas asumidas de la globalización ponen en cuestionamiento los conceptos tradicionales y las prácticas, las epistémicas o conocimientos dominantes en América Latina y hay necesidad de pensar en una teoría crítica que sea auténticamente periférica, que parta del *Sur* y que tenga en cuenta esa teoría crítica los procesos políticos, las dinámicas sociales en América Latina.[282]

Esta propuesta demanda la articulación de conocimientos legales, herramientas digitales y prácticas sociales, generando estrategias que valoren la realidad, para abordar el impacto provocado en entornos virtuales se requiere de una normativa con enfoque restaurativo, orientado a reparar daños provocados por la tecnología. Además de una formación crítica, que fortalezca la autonomía colectiva frente a contenidos manipulados, por tanto, la respuesta debe ser sensible y orientada a contextos situados en la realidad social.

Finalmente, si bien la tecnología *deepfake* se trata de un desafío significativo, existen tecnologías como "Blockchain para proporcionar una validación descentralizada de la autenticidad y una clara cadena de custodia que sea potencialmente efectiva como una herramienta para rastrear y verificar no solo los recursos financieros, sino todo tipo de formas de contenido".[283] La tecnología blockchain permite registrar la huella digital de contenido original verificando su autenticidad con versiones almacenadas ayuda a detectar si un video o imagen ha sido alterado.

[282] Antonio Carlos Wolkmer, "La crítica jurídica latinoamericana", video de Youtube, entrevista presentada a la Universidad Andina Simón Bolívar, 2014, 8:00, https://n9.cl/go8ne.

[283] Nadia Hewett y Karin Gabriel, "Blockchain puede ayudar a combatir la amenaza de los deepfakes", *World Economic Forum,* Accedido 6 de septiembre de 2025, párr. 12, https://www.weforum.org/stories/2021/10/how-blockchain-can-help-combat-threat-of-deepfakes/.

Conclusiones

En conclusión, la IA se trata de una tecnología innovadora, que puede mejorar la sociedad en distintas áreas. Pero cuando se utiliza, sin una regulación ni principios éticos que guíen su uso, representa un riesgo para los derechos fundamentales. En el caso de los *deepfakes* pornográficos, amplifican los daños debido a su validación a través de mecanismos de ingeniería social que distorsionan la realidad. La apropiación no consentida de imágenes convierte a las personas en objetos de consumo, vulnerando su dignidad y afectando su esfera íntima, familiar, social y profesional. Frente a este fenómeno, se requiere construir marcos normativos multidisciplinarios que respondan de manera técnica y con eficacia a los desafíos de esta nueva realidad digital.

Desde una perspectiva social, se concluye que los *deepfakes* pornográficos constituyen una conducta dañina que vulnera los derechos fundamentales vinculados a la dignidad humana. Y aunque en sus inicios estas agresiones digitales se dirigieron a figuras del espectáculo, también pueden afectar a personas particulares. En cuanto a su aumento, desde el año 2019, ha experimentó una expansión de 550 % a nivel global, y a nivel nacional se registra un crecimiento de 441 %. Si bien es cierto, cualquier persona puede ser víctima de la creación y difusión de *deepfakes* pornográficos, las cifras porcentuales revelan una modalidad específica de violencia digital con sesgo de género.

Asimismo, desde la perspectiva social se concluye que el *soft law* sustentado en principios orientadores y programas de educación digital, constituye una herramienta para prevenir vulneraciones y orientar el uso responsable de aplicaciones y plataformas digitales. Se trata de un complemento al marco jurídico formal permitiendo actuar con mayor agilidad cuando la tecnología avanza más rápido que el derecho, influyendo en la toma de decisiones dentro del entorno virtual, sin depender exclusivamente de reformas legislativas que suelen ser lentas y complejas. Se trata de un mecanismo adaptativo, que parte de la educación y se proyecta hacia el ámbito social, fomentando una cultura digital respetuosa de los derechos fundamentales, sin obstaculizar la innovación tecnológica.

En el ámbito del derecho, se concluye que la fase administrativa ofrece rutas de contención y reparación, como se evidencia en los dos casos de estudio seleccionados. En el primero, la omisión del protocolo por parte del establecimiento vulneró gravemente los derechos de una estudiante menor de edad, sin activar mecanismos institucionales de protección ni garantizar atención psicosocial. En el segundo, la universidad debió activar

su autonomía para garantizar un proceso imparcial frente a la afectación, evidenciando que el abordaje de este problema exige respuestas institucionales sensibles y eficaces. En ambos casos, la violencia no sólo es digital sino también institucional, por la omisión de las autoridades. De esta manera el protocolo de actuación activar medidas urgentes, sin embargo, él mismo debe implementar reformas que aborden las nuevas formas de violencia digital.

Se concluye que una posible solución en el ámbito judicial civil ecuatoriano frente a estos hechos es la acción por daños y perjuicios, que permite reclamar la afectación provocada por contenidos digitales como los *deepfakes* de índole sexual. En ambos casos analizados, se evidenció una afectación emocional profunda, por lo que el daño principal fue de carácter moral, al comprometer la esfera psicológica, reputacional e íntima de las víctimas. En este contexto, corresponde una indemnización económica como parte de una reparación que reconozca el sufrimiento causado y contribuya a mitigar sus efectos. Esta vía, aunque limitada frente a la complejidad tecnológica, se convierte en un recurso legítimo para exigir justicia material y de carácter pecuniario.

En conclusión, el habeas data se configura como la garantía constitucional más idónea para la protección de los derechos vulnerados por *deepfakes* pornográficos no consentidos. Su aplicación permite tutelar los datos personales, activar medidas de reparación integral y detener la circulación de contenidos digitales que afectan la dignidad, la intimidad y la imagen de las personas. Tal como lo sostiene el experto en derecho constitucional Cristian Masapanta, y conforme a lo establecido en la sentencia Nº 2064-14-EP/21 de la Corte Constitucional, el alcance de esta garantía puede ampliarse mediante interpretación constitucional, adaptándose a los desafíos tecnológicos contemporáneos como la inteligencia artificial generativa, la manipulación algorítmica y el reconocimiento automatizado de la imagen digital.

De la misma manera, se concluye que los *deepfakes* evidencian la intersección entre los derechos de autor y los derechos de la personalidad y puede ser considerados parodias siempre que conserven un carácter humorístico y se ajusten a las normas de protección de datos. Sin embargo, se convierten en infracciones cuando vulneran obras protegidas o afectan la identidad de las personas. Además, los *deepfakes* muestran datos e imágenes sintéticas que al ser demasiado realistas tienden a poner en riesgo la dignidad de la persona. Por ello, el habeas data y las normas sobre tratamiento de datos personales podrían constituir herramientas esenciales para enfrentar estos riesgos evitando posibles vulneraciones a los derechos fundamentales.

En conclusión, el mundo digital es una extensión de nuestra realidad, lo que es punible en el mundo físico también debería ser punible en el entorno virtual. Sin embargo, resulta un obstáculo la falta de adaptación de las normas tradicionales a las nuevas circunstancias de violencia digital. En Ecuador, la falta de una regulación específica ha causado la impunidad en casos como el de Sofía o Simón (seudónimos), por esta razón la implementación de tecnologías capaces de detectar contenidos manipulados en tiempo real podría constituir una respuesta estratégica. Las herramientas como la tecnología *blockchain* o el etiquetado ofrecen alternativas inmediatas y aplicables, mientras se consolidan marcos normativos que puedan ser aplicables a la realidad actual.

Sin embargo, se concluye que la obligación de etiquetar un contenido como generado por inteligencia artificial es insuficiente, pues el sólo señalamiento no ofrece una proteccion de manera efectiva de los derechos fundamentales de las personas. Así como lo ha señalado el experto en cibercrímenes Santiago Acurio, resulta imprescindible la tipificación de un tipo penal autónomo que sancione los *deepfakes* pornográficos generados mediante IA, dado que esta práctica vulnera de manera grave el bien jurídico de la dignidad humana y ocasiona daños irreparables a las personas afectadas. En consecuencia, la regulación debe contemplar penas privativas de libertad, sanciones pecuniarias y la implementación de mecanismos de protección integral que garanticen la defensa efectiva de las víctimas frente a este fenómeno digital.

En conclusión, es fundamental que la ciudadanía en general utilice responsablemente las nuevas tecnologías, especialmente la IA. En ese contexto, la alfabetización digital es clave para prevenir vulneraciones y proteger la dignidad humana. Al alcanzar un punto donde las capacidades de cada estado para el control de esta situación sean insuficientes, se plantea la integración regional como una solución que puede ofrecer respuestas coordinadas, adaptadas a cada realidad superando las limitaciones estatales. Según la opinión del experto Ibán García del Blanco, la Unión Europea podría servir como referente al implementar normativas como el Reglamento de IA, la Oficina de IA y el Digital Services Act, se trata de organismos y reglamentos que sancionan el uso dañino de la IA, articulando innovación tecnológica con protección de derechos fundamentales.

Bibliografía

Abril, Rubén. “Neuronas de McCulloch y Pitts Artículo de LMO”. *La Máquina Oráculo*. Accedido 19 de mayo de 2025. https://n9.cl/6jdgc.

Agencia Española de Protección de Datos. “Datos sintéticos y protección de datos”, *AEPD*. Accedido 23 de enero de 2026. https://www.aepd.es/prensa-y-comunicacion/blog/datos-sinteticos-y-proteccion-de-datos.

Albán Alencastro, Juan Pablo, Valeria Betancourt, Hugo Cahueñas Muñoz, Arturo Carrillo, Andrés Delgado, Sophia Espinosa Coloma, Gustavo Gómez, et al. *Regulación del Internet y derechos digitales en Ecuador*. Quito: Editorial USFQ, 2016.

Alexander, George, y Andrew Bennet. *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press, 2005.

Alfabetización Audiovisual. “Ética Digital y Buenas Prácticas en la Producción y Distribución de Contenido Audiovisual”. *Alfabetización Audiovisual*. Accedido 18 de septiembre de 2025. https://acortar.link/IgAONJ.

Andino Vélez, Byron. “Deepfake, cinismo y diversión en la crueldad: Un caso de colegiales y pornografía en Ecuador”. *Uru: Revista de Comunicación y Cultura* 11, n.° 2 (2025): 8–28. doi:10.32719/26312514.2025.11.2.

Atienza, Manuel. *Sobre la dignidad humana*. Madrid: Trotta, 2022.

Azuaje Pirela, Michelle. “Deepfakes, distorsión de la realidad y desafíos jurídicos”. *Telos Fundación Teléfonica*. Accedido 2 de septiembre de 2025. https://acortar.link/vuGQyG.

Ballesteros-Aguayo, Lucia, y Francisco Javier Ruiz Del Olmo. “Vídeos Falsos y Desinformación Ante la IA: el Deepfake como Vehículo de la Posverdad”. *Revista de Ciencias de la Comunicación e Información* 29, n.° 1 (2024): 1–14. doi:10.35742/rcci.2024.29. e294.

Bañuelos Capistrán, Jacob. “Deepfake: la imagen en tiempos de la posverdad”. *Revista Panamericana de Comunicación* 2, n.° 1 (2020): 51–61. doi:10.21555/rpc.v0i1.2315.

———. “Evolución del Deepfake: campos semánticos y géneros discursivos 2017-2021”. *Revista ICONO 14. Revista científica de Comunicación y Tecnologías emergentes* 20, n.° 1 (2022): 21. doi:10.7195/ri14.v20i1.1773.

Barba Arteaga, Cecilia. “Deepfakes sexuales: impacto, prevención y perspectivas de género en el entorno digital”. *Miguel Hernández Communication Journal* 15, n.° 2 (2024): 9. doi: https://doi.org/10.21134/zt4eht31.

Barfield, Woodrow. *The Cambridge Handbook of the Law of Algorithms*. Cambridge: Cambridge University Press, 2020.

Barrio Andrés, Moisés. “Génesis y desarrollo de los derechos digitales”. *Revista de las Cortes Generales* 6, n.° 10 (2021): 11. doi:10.33426/rcg/2021/110/1572.

———. *Los Derechos Digitales y su Regulación en España, la Unión Europea e Iberoamérica*. Madrid: Colex, 2023.

Bauman, Zygmunt. *Modernidad Líquida*. Madrid: Fondo de Cultura Económica de España, 2000.

Bayo Pérez, Blanca. “Los deepfakes pornográficos aumentan un 464% con la mujer como víctima principal”. *Verifica RTVE*. Accedido 1 de octubre de 2025. https://acortar.link/2SLFi8.

BBC News Mundo. “Instagram: más de 40 estados en EE.UU. demandan a la red social por supuestos daños en la salud mental de los adolescentes”. *BBC News Mundo*. Accedido 30 de agosto de 2025. https://acortar.link/vhFcSC.

Belda, Ignasi. *Inteligencia Artificial*. Barcelona: RBA Coleccionabes, S.A, 2019.

Benjamín, Walter. *La obra de arte en la época de su reproductibilidad técnica.* Buenos Aires: Taurus, 1989.

Bhaskar, Michael, y Camila Rocca. “La Inteligencia Artificial y las editoriales”. *Trama Editorial* 12, n.° 44 (2025): 4. doi:190.216.103.250.

Bigas Fortmajé, Núria. “Deepfake pornográficos”. *Universitat Oberta de Catalunya (UOC)*. Accedido 11 de julio de 2025. https://n9.cl/9iu39.

Boté Vericad, Juan José, y Mari Vállez. “Aplicaciones de deepfakes. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad”. *Documentación de las Ciencias de la Información* 45, n.° 1 (2022): 25–32. doi:10.5209/dcin.77256.

Briefing, China. “Comprender las nuevas regulaciones de China sobre IA generativa”. *China Briefing News*. Accedido 13 de julio de 2025. https://n9.cl/twop7.

Brownlee, Jason. *Generative Adversarial Networks with Python*. Melbourne: Machine Learning Mastery, 2021.

Bud, Andrew. “Menos del 1% de falsificaciones generadas por IA se detectan: iProov - Revista Mas Seguridad”. *Revista Mas Seguridad*. Accedido 4 de septiembre de 2025. https://n9.cl/8ydyfr.

Bussines, Wire. “iProov Study Reveals Deepfake Blindspot: Only 0.1% of People Can Accurately Detect AI-Generated Deepfakes - Silicon Canals”. *Silicon Canals*. Accedido 7 de julio de 2025. https://n9.cl/gth4s1.

Camacho, Miguel. “Historia y Computación: Estudiar el pasado con los medios más modernos”. *Historia y Espacio* 2, nº 15 (2018): 143–66. doi:10.25100/hye.v0i15.6886.

Casabo Ortíz, María de los Ángeles. “Víctimas menores de edad por revenge porn: protección jurídica ante los riesgos del “internet inseguro”. *Revista Electrónica de Ciencias Criminológicas* 6, nº 7 (2022): 23–25. https://hdl.handle.net/10550/93007.

CaseGuard. “Australia evalúa nuevas normas sobre reconocimiento facial”. *AI Redaction & Privacy for All*. Accedido 10 de octubre de 2025. https://n9.cl/266k0.

Castillo, Gonzalo. “Qué es Digital Content: tipos, funciones y ejemplos”. *InnovaciónDigital360*. Accedido 2 de septiembre de 2025. https://n9.cl/bqjla.

Cerdán Martínez, Víctor, María Luisa García Guardia, y Graciela Padilla Castillo. “Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales”. *CIC. Cuadernos de Información y Comunicación* 2, n.° 25 (2020): 165–81. doi:10.5209/ciyc.68762.

Climent Gallard, Jorge Antonio. “Los deepfakes satíricos o paródicos: análisis desde la perspectiva del derecho europeo”, *Revista Boliviana de Derecho* 2, nº 39 (2025): 62, https://n9.cl/u1lt5.

Coeckelberg, Mark. *Ética de la inteligencia artificial*. Madrid: Ediciones Cátedra, 2021.

Córdova, Ximena. “El aumento de los deepfakes criminales: fraude, pornografía y suplantación de identidad”. *Diario El Imparcial*. Accedido 31 de agosto de 2025. https://acortar.link/MYDMsD.

Cortés Rodas, Francisco. “El contrato social en Hobbes: ¿absolutista o liberal?”. *Estudios Políticos del Instituto de Estudios Políticos de la Universidad de Antioquia* 5, n.° 37 (2010): doi: https://doi.org/10.17533/udea.espo.8072.

Cortina, Adela. *¿Ética o ideología de la inteligencia artificial? El eclipse de la razón comunicativa en una sociedad tecnologizada.* España: PAIDÓS, 2024.

Crespo, Roberto. “Transformer: Attention is all you need”. *Tecnología, marketing digital y desarrollo personal*. Accedido 24 de agosto de 2025. https://acortar.link/Boxr3z.

De Jong, Koen. “El poder de ViT, Transformadores de Visión para el Reconocimiento de Imágenes”. *Visionplatform.ia*. Accedido 25 de agosto de 2025. https://acortar.link/vhakyW.

Decide Soluciones. “IA Generativa: qué es, historia, tipos y casos de uso”. *Decide Soluciones*. Accedido 3 de septiembre de 2025. https://n9.cl/lmci5p.

Dialoguemos. “Nueva York demandó a cinco redes sociales por la crisis de salud mental en niños y jóvenes”. *Dialoguemos. La academia en la comunidad*. Accedido 30 de agosto de 2025. https://acortar.link/Sc2cmj.

Díaz Ramírez, Jorge. “Aprendizaje Automático y Aprendizaje Profundo”. *Ingeniare. Revista chilena de ingeniería* 29, nº 2 (2021): 180–81. doi:10.4067/S0718-33052021000200180.

Dromi, Roberto. *Derecho Administrativo*. Lima: Gaceta Jurídica, 2005.

Dunbar, Graham. “FIFA multa a Argentina y otras selecciones por racismo de hinchas en eliminatorias”. *Independent en español*. Accedido 9 de septiembre de 2025. https://n9.cl/vtcea.

Espinosa Carvajal, Geovanna Gabriela, y Fernando Eduardo Paredes Fuentes. “Los ciber delitos y la protección de datos personales en el sistema penal ecuatoriano”. *Revista Lex* 8, n.° 29 (2025): 559–72. doi:10.33996/revistalex.v9i28.302.

Espinoza Andrade, Yandri Jesús, Manuel Fernando Heredia Arias, Ronal Antonio Benavides Ortega, y Xiomara Belén Sanjinés Domínguez. “Evolución del Manejo de las TIC en la Informática y su Impacto en el Uso de Recursos Informáticos”. *Ciencia Latina Revista Científica Multidisciplinar* 8, n.° 4 (2024): 1–10. doi:10.37811/cl_rcm. v8i4.12482.

Fanni, Simona. “La inteligencia artificial y el cuerpo humano digital: a la búsqueda del habeas data.” *IUS ET SCIENTIA* 6, n.° 2 (2020): 180. doi:10.12795/IETSCIENTIA. 2020.i02.13.

Fernández, Antonio, Daniel Fernández, Diana Molero, Miguel Àngel Pérez, Beatriz García, Marta Barroso, y Lydia García. *Deepfakes: Riesgos, Casos Reales y Desafíos en la Era de la IA*. Madrid: Observatorio de Deepfake del ISMS Forum, 2025. https://www.ismsforum.es/ficheros/descargas/deepfake-final1742458135.pdf.

Fernández, Maximiliano. “El milagroso (o perturbador) algoritmo de TikTok: qué hay detrás de la red social más adictiva”. *Infobae*. Accedido 4 de septiembre de 2025. https://n9.cl/bkb6t.

Fischer, Brendan. “Newly Published Cambridge Analytica Documents Show Unlawful Support for Trump in 2016”. *Campaign Legal Center*. Accedido 4 de septiembre de 2025. https://n9.cl/mrrkh9.

Floridi, Luciano. *Ética de la inteligencia artificial*. Barcelona: Herder, 2023.

Franganillo, Jorge. “La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos”, *Methaodos revista de ciencias sociales* 11, nº 2 (2023): 9-12. doi:10.17502/mrcs.v11i2.710.

Galperin, Hernán. *Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe*. París: UNESCO Programa MOST, 2017.

Gandhi, Kashish, Prutha Kulkarni, Taran Shah, Piyush Chaudhari, Meera Narvekar, y Kranti Ghag. “A Multimodal Framework for Deepfake Detection”. *Journal of Electrical Systems* 20, nº 10 (2024): 85. https://n9.cl/nsz1fh.

García Falconí, José Carlos. *La Demanda Civil de Daños y Perjuicios y Daño Moral por Responsabilidad Subjetiva en contra de los Jueces, Fiscales y Defensores Públicos*. Quito: Ediciones Rodin, 2010.

García Jiménez, Antonio, y Beatriz Catalina García. “Una perspectiva documental y bibliotecológica sobre el big data y el periodismo de datos”. *Investigación Bibliotecológica: archivonomía, bibliotecología e información* 32, nº 74 (2018): 77. doi:10.22201/iibi.24488321xe.2018.74.57910.

Gil de la Guardia, Alberto. “Inteligencia Artificial: La Revolución que acelera más rápido que la humanidad puede adaptarse”. *sección artículos de LinkedIn*. Accedido 2 de septiembre de 2025. https://n9.cl/qj7cgx.

Gilchrist, Alan Duncan. “From Punched Cards to Google: An Outline History of Information Retrieval”. *Scire: Representación y Organización Del Conocimiento* 24, n.˚ 1 (2018): 13–21. doi:10.54886/scire.v24i1.4598.

GIRHA TEC. “GANs: La Tecnología Revolucionaria Detrás de los Deepfakes”. *GIRHA TEC*, Accedido 20 de julio de 2025. https://n9.cl/oxyd5i.

Glaser, Barney, y Anselm Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company, 1967.

Godoy, Lorena Naranjo. “Aproximación a la categorización de derechos digitales y su aplicación en Ecuador”. *Revista Cálamo* 5, n.° 21 (2024): 7. doi:10.61243/calamo.21.423.

Gómez Robledo Verduzco, Alonso. *El derecho a la intimidad y el derecho a la libertad de expresión: Derechos humanos fundamentales*. San José: Corte Interamericana de Derechos Humanos, 2015.

Harari, Yuval Noah. *Nexus: A Brief History of Information Networks from the Stone Age to AI*. Barcelona: Debate, 2024.

Hernández Guerra, Arnaldo. “La persona hiperconectada: reflexiones desde el desarrollo humano, enfoque centrado en la persona”. *Revista Comunicación* 30, n.° 2 (2021): 46–59. doi:10.18845/rc.v30i2-2021.6030.

Hernández, Helena. “Los ‘deepfakes’ y el derecho penal”. *Ámbito Jurídico*. Accedido 10 de septiembre de 2025. https://n9.cl/xo2g7.

Herrera González, Isabel. “Democratización de la tecnología: emisores contemporáneos”. *El Pájaro de Benín* 1, nº 8 (2022): 111–26. doi:10.12795/pajaro_benin. 2022.i8.05.

Hewett, Nadia y Karin Gabriel. “Blockchain puede ayudar a combatir la amenaza de los deepfakes”. *World Economic Forum,* Accedido 06 de septiembre de 2025. https://n9.cl/gyvon.

Jara Holliday, Oscar. *La sistematización de experiencias: práctica y teoría para otros mundos posibles*. Bogotá: Centro Internacional de Educación y Desarrollo Humano, 2018.

Koppen Prubmann, Elke. “Photoforensics y el análisis de imágenes digitales”. En *La fotografía en el contexto del cambio: retos y perspectivas*, editado por Héctor Guillermo Alfaro López y Graciela Leticia Raya Alonso, 16-25. Ciudad de México, UNAM: Universidad Nacional Autónoma de México, 2019.

León Batista, Hernán Antonio. “La dignidad humana en la era digital”. *Anuario de Derecho Constitucional Latinoamericano 26*, n.° 8 (2020): 2. https://biblio.juridicas.unam.mx/bjv.

Llamas Covarrubias, Jersain Zadamig, Olivia Andrea Mendoza Enríquez, y Mario Graff Guerrero. “Enfoques regulatorios para la Inteligencia Artificial (IA)”. *Revista Chilena de Derecho* 49, n.° 3 (2022): 10. doi:10.7764/R.493.2.

López Rincón, Gustavo Andrés, y Laura Marcela Quintero Sánchez. “Delitos contra la intimidad personal en el marco de la inteligencia artificial en Colombia”.

Postulados: Revista Sociojurídica 1, nº 2 (2025): 57. doi:10.22463/29816866.4300.

Lyon, Bryan, y Matt Tora. *Exploring Deepfakes*. Birmingham: Packt Publishing, 2023.

Manckenzie, Jean. "La crisis del porno deepfake que afecta a las escuelas coreanas". *BBC News Mundo*. Accedido 30 de agosto de 2025. https://n9.cl/po2mp.

Martínez, Alonso. "Take it Down Act, la ley que criminaliza los deepfakes y la pornovenganza". *El País US*, Accedido 20 de mayo de 2025. https://n9.cl/x2xl7.

Martínez Pérez, Odette, Edward Fabricio Freire Gaibor, y Luis Alberto Alzate Peralta. "Desafíos del habeas data en la protección de datos personales en el ordenamiento jurídico ecuatoriano". *European Public & Social Innovation Review* 2, nº 9 (2024): 1–21. doi:10.31637/epsir-2024-1842.

McDermott, Sarah, y Jess Davies. "Deepfake: 'Pusieron mi cara en un video porno'". *BBC News Mundo*. Accedido 25 de julio de 2025. https://n9.cl/iqx5h.

Micucci, Mario. "Herramientas para detectar deepfakes y combatir la desinformación". *welivesecurity*. Accedido 11 de octubre de 2025. https://n9.cl/t4cnto.

Mikkelson, Stephanie, Emily Springer, y Nora Piay Fernandez. *An infographic guide to an infographic guide to TFGBV*. New York: UNFPA, 2025.

Mishra, Ranjan Kumar, Sandesh Reddy, y Himanshu Pathak. "The Understanding of Deep Learning: A Comprehensive Review". *Mathematical Problems in Engineering* 5, nº 1 (2021): 2. doi:10.1155/2021/5548884.

Mondragón Duarte, Sergio, Sergio Caballero, Leonardo Díaz, Johana Herrera. "Protección jurídica de los derechos de autor en Colombia". *SUMMA. Revista disciplinaria en ciencias económicas y sociales* 4, nº 1 (2022): 3–6. doi:10.47666/summa.4.1.09.

Molina Bolívar, Camilo, Amparo Cadavid, Fernando Casado, Ana María Durán, y Eduardo Gutiérrez. "La Comunicación y su impacto en la vida democrática de América Latina y el Caribe". *Chasqui: Revista Latinoamericana de Comunicación* 19, n.° 141 (2019): 27. file:///C:/Users/cango/Downloads/REXTN-Ch146.pdf.

Morales Luna, Guillermo. "La criptología y la victoria aliada en la Segunda Guerra Mundial". *Revista Ciencia* 64, n.° 4 (2013): 3. doi: 10.25186/rev.ciencia.2013.4.6886.

Morales Ordoñez, Juan. *Ética Y Sociedad*. Cuenca: Universidad del Azuay, 2008.

Moreta, Andrés. *Procedimiento Administrativo y Sancionador en el COA*. Quito: Ediciones Continente, 2019.

Muñoz del Alba Medrano, Marcía. *Habeas Data*. Ciudad de México: Instituto de Investigaciones Jurídicas UNAM, 2006.

Napolitan, Richard, y Xia Jiang. *Artificial Intelligence with an Introduction to Machine Learning*. New York: Taylor & Francis Group, 2018.

Oliver, Nuria. *INTELIGENCIA ARTIFICIAL*. Madrid: Ministerio de Asuntos Económicos y Transformación Digital, 2021.

ONU. "Derechos humanos en la era digital". *Organización de Naciones Unida.* Accedido 7 de agosto de 2025. https://www.ohchr.org/es/2019/10/human-rights-digital-age.

Orellana Robalino, Claudia. "De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales." *FORO Revista de Derecho,* n. º 27 (2017): 7. https://revistas.uasb.edu.ec/index.php/foro/article/view/498/485.

Ortega Hernández, Carmen Carolina, Norma Esther López Maldonado, y Teresa Del Carmen Cabrera Gómez. "Violencia digital y afectiva en redes sociales". *Transdigital* 5, nº 10 (2024): e374. doi:10.56162/transdigital374.

Oviedo Fadul, Alexander. *Diseño estructurado de algoritmos*. Sincelejo: Imprenor, 2004.

Páez Rivadeneira, Juan José, y Santiago Acurio del Pino. *Derecho y Nuevas Tecnologías*. Quito: Corporación de Estudios y Publicaciones CEP, 2010.

Páez Salgado, Daniela. "¿Daño moral por incumplimiento de contrato?" *Iuris Dictio* 14, nº 16 (2015): 24. doi:10.18272/iu. v14i16.729.

Palazzi, Pablo. *Delitos Informáticos*. Buenos Aires: AD-HOC Sociedad de Responsabilidad Limitada, 2000.

Patton, Michael. *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. California: SAGE Publications, 2014.

Peña, Renata Correa. "Delito de Deepfake y Pornografía Infantil Generada por Inteligencia Artificial (IA) en la Legislación Ecuatoriana". Tesis académica, Universidad Católica de Cuenca, 2024. https://n9.cl/a63mf0.

Pereira Hernández, María Luisa, y Virginia Mirella Zatarain Avendaño. "Pornografía deepfake en la era de la IA: nuevos desafíos para la educación de género, humanística y tecnológica". *RECIE. Revista Electrónica Científica de Investigación Educativa* 8, n.˚ 10 (2024): 3. doi:10.33010/recie. v8i0.2337.

Pérez Cázares, Martín Eduardo. “El habeas data o derecho a la intimidad en el derecho informático”. *Revista del Instituto de Investigaciones Legislativas del Congreso del Estado de México* 15, nº 98 (2021): 2. https://n9.cl/xrlvp.

Polo, Nathalia. “IA contra deepfakes al vuelo: el escudo digital de 2025”. *WhatsNew*. Accedido 16 de septiembre de 2025. https://n9.cl/8ob5n.

Ponce Cedeño, Angie Dayana, Génesis Karolina Robles Zambrano, y Ingrid Joselyne Díaz Basurto. “La inteligencia artificial y el derecho a la intimidad-privacidad”. *IUSTITIA SOCIALIS* 8, nº 1 (2023): 84–93. doi:10.35381/racji.v8i1.2493.

Prado, Gabriela Prado, y Mario Durán Migliardi. “Sobre la evolución de la protección penal de los bienes jurídicos supraindividuales. Precisiones y limitaciones previas para una propuesta de protección penal del orden público económico en Chile”. *Revista de Derecho Universidad Católica del Norte* 24, nº 1 (2017): 263–95. doi:http://dx.doi.org/10.4067/S0718-97532017000100263.

Presno Linera, Miguel Ángel. *Derechos fundamentales e inteligencia artificial*. Madrid: Marcial Pons, 2022.

Proaño, Pamela. “¿Ciberseguridad en Ecuador? Deepfakes, ransomware y lo que no estás viendo”. *Equinoccio Digital*, 12 de junio de 2025. https://n9.cl/7nh5n.

RAE. “pornografía”. *Real Academía Española*. Accedido 18 de septiembre de 2025. https://www.rae.es/diccionario-estudiante/pornografía.

Ramos-Zaga, Fernando. “Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial”. *Derecho Global. Estudios sobre Derecho y Justicia* 9, nº 27 (2024): 359–87. doi:10.32870/dgedj.v9i27.754.

Redacción EFE. “Los deepfakes, creaciones digitales usadas para perjudicar a mujeres con videos pornográficos falsos”. *El Universo*. Accedido 14 de octubre de 2025. https://n9.cl/uuit91.

Regan, Gabe. “Una breve historia de Deepfakes”. *Reality Defender*. Accedido 8 de junio de 2025. https://n9.cl/nyk8d.

Rico Carrillo, Mariliana. *Derecho de las nuevas tecnologías*. Buenos Aires: Ediciones La Roca, 2007.

Rosado García, Tania Lisseth, Maria Magdalena Chancay Chancay, Tony Paul Alcivar Vera, Alex Andres Acosta Marino, Angelica Alexandra Cobena Cedeno, y Carlos Julio Bernal Mendieta. “Development of ethical values in digital education”. *Universidad Ciencia y Tecnología* 29, n.° 8 (2025): 114–23. doi:10.47460/uct.v29iSpecial.885.

Rueda Fonseca, María del Socorro. “Las Vertientes Doctrinarias Del Daño Moral O Pretium Doloris”. *Revista Boliviana de Derecho* 10, n.° 4 (2007): 20. http://www.redalyc.org/articulo.oa?id=427539904003.

Sanabria Navarro, José Ramón, Yahilina Silveira-Pérez, Digna Dionisia Pérez Bravo, y Manuel de Jesús Cortina Núñez. “Incidencias de la inteligencia artificial en la educación contemporánea”. *Comunicar* 31, n.° 77 (2023): 8. doi:10.3916/C77-2023-08.

Sánchez Zambrano, José, Inés Guamán Lema, y Pedro Peñafiel Fárez. “Daños y Perjuicios y Daño Moral en el Sistema Procesal Ecuatoriano”. *Derecho Crítico: Revista Jurídica, Ciencias Sociales y Políticas* 8, n° 3 (2023): 9. doi:10.53591/dcjcsp.v3i3.1095.

Santistevan Villacreses, Karina Lourdes, Johanna Lissette Arias Haro, y Sandy Briggette Sánchez Chávez. “Las plataformas digitales y su impacto en las ventas de las pequeñas empresa del cantón Paján”. *Revista Estudios del Desarrollo Social: Cuba y América Latina* 8, n.° 1 (2022): 6–15. doi:10.5281/zenodo.8383401.

Serpa, Cecilia. “Escritura y Derecho: la narración de hechos desde una perspectiva sistémico-funcional”. *Revista de la Facultad de Derecho de México* 7, n.° 28 (2023): 5. doi:10.22201/fder.24488933e.2023.285.85404.

Sharma, Preeti, Manoj Kumar, Hitesh Kumar Sharma, y Soly Mathew Biju. “Generative adversarial networks (GANs): Introduction, Taxonomy, Variants, Limitations, and Applications”. *Multimedia Tools and Applications* 83, n.° 41 (2024): 2–3. doi:10.1007/s11042-024-18767-y.

Simón Soler, Elisa. “Retos jurídicos derivados de la Inteligencia Artificial Generativa”. *InDret* 2, n.° 12 (2023): 6. doi:10.31009/indret. 2023.i2.11.

Sinaluisa Sagñay, Franklin Geovanny, Wendy Pilar Romero Noboa, y Nelson Francisco Freire. “Deepfakes Pornográficos: Impacto jurídico-probatorio y social en el Ecuador”. *Reincisol* 3, n.° 6 (2024): 1–23. doi:10.59282/reincisol.V3(6)2912-2934.

Solar Cayón, José Ignacio, y Olga Sánchez Martínez. *El impacto de la inteligencia artificial en la teoría y la práctica jurídica*. Madrid, España: Wolters Kluwer Legal & Regulatory España, 2022.

Teijón Alcalá, Marco. “El deepfake pornográfico: concepto y alcance penal”. *Anuario de la Facultad de Derecho de la Universidad de Alcalá* 7, nº 17 (2024). doi:10.14679/3901.

The Black Box Lab. “Deepfakes: La Realidad Transformada, Tipos y Aplicaciones”. *The Black Box Lab*. Accedido 2 de septiembre de 2025. https://theblackboxlab.com/deepfakes/.

Tobar, Estefany Alvear, y Nicole Enríquez Espinoza. “Tipos penales para conductas que vulneran la integridad sexual, a través del mal uso de inteligencia artificial en Ecuador”. *Derecho Penal Central* 5, n.° 6 (2025): 9. doi:10.29166/dpc.v6i6.7701.

Toro Huerta, Mauricio Iván Del. “El fenómeno del soft law y las nuevas perspectivas del derecho internacional”. *Anuario Mexicano de Derecho Internacional* 1, n.° 6 (2006): 1–38. doi:10.22201/iij.24487872e.2006.6.160.

Torres Ruiz, Angela Esther. “El transitar en la investigación cualitativa: un acercamiento a la triangulación”. *Revista Scientific* 6, n.° 20 (2021): 275–95. doi:10.29394/Scientific.issn.2542-2987.2021.6.20.15.275-295.

UAC. “Teoría del delito. Evolución. Elementos Integrantes”. *Universidad Andina del Cusco, Perú*, 15 de junio de 2018, núm. 29, https://n9.cl/u1d42.

Ultralytics. “La autoatención explicada”. *Ultralytics*. Accedido 2 de septiembre de 2025. https://www.ultralytics.com/es/glossary/self-attention.

Urbina Carvajal, Gloria Rosana, Mariela Verónica Bernita Peñafiel, Galia Jennis Véliz Castillo, y Ángel Leonardo Bermúdez Mendoza. “Evolución y Aplicación de la Teoría del Delito en el Sistema Penal Ecuatoriano”. *LexEnlace Revista Científica Jurídica* 1, nº 2 (2024): 9. https://lexenlace.com/wp-content/uploads/2024/12/LEX-AC77.pdf.

Varona, Gema, Ignacio José Subijana Zunzunegui, Ana Eugenia Abasolo Telleria, Itziar Altuzarra Alonso, Silvia Badiola, Menchu Bernal, Mireia Elizetxea López, et al. *Victimología Didáctica y Aplicada: Análisis de Casos*. Madrid: Laborum Ediciones, 2025. https://n9.cl/q7w0r.

Vázquez, Daniel, y Horacio Ortiz. “Impunidad, corrupción y derechos humanos”. *Perfiles Latinoamericanos* 29, n.° 57 (2021): 1–28. doi:10.18504/pl2957-007-2021.

Velasco Núñez, Eloy. *Delitos tecnológicos Cuestiones penales y procesales*. Madrid, España: Wolters Kluwer S.A., 2021.

Vide, Carlos Rogel. “Origen y actualidad de los derechos de la personalidad”. *REVISTA IUS* 1, nº 20 (2017): 7-10. doi:10.35487/rius. v1i20.2007.278

Vilches, Ignacio Carrascón, Sandra. "¿Qué hace falta para que tus ojos vean algo que nunca ocurrió? Así se crean los 'deepfakes' en vídeo y en imagen". *Newtral*. Accedido 16 de mayo de 2025. https://n9.cl/jwuxp.

Vinelli Vereau, Renzo Antonio. "Los delitos informáticos y su relación con la criminalidad económica". *Ius et Praxis*, nº 1 (2021): 95–110. doi:10.26439/iusetpraxis2021.n053.4995.

Willians, Guido. *Conceptos de soft law, hard law, better regulation, smart regulation y políticas públicas*. Asesoría técnica. Chile: Biblioteca del Congreso Nacional de Chile, 2021. https://n9.cl/m46cm.

Wolkmer, Antonio Carlos. "La crítica jurídica latinoamericana". Video de Youtube, a partir de una entrevista presentada a la Universidad Andina Simón Bolívar, Sede Ecuador, 2014. https://n9.cl/go8ne.

Zaffaroni, Eugenio Raúl. *La palabra de los muertos: conferencias de criminología cautelar*. Quito: Editorial El Siglo, 2018.

Zavala Egas, Jorge, María Josefa Coronel, Rafael Bigrante Guerra, Jorge Egas Peña, Miguel Hernández Terán, Gonzalo Noboa Baquerizo, Ernesto Velásquez Baquerizo, et al. *Homenaje Póstumo al Dr. Edmundo Durán Díaz*. Quito: Revista Jurídica de la Universidad de los Hemisferios, 2002.

Zill, Dennis, y Warren Wright. *Matemáticas 1: cálculo diferencial*. Ciudad de México: McGraw-Hill Interamericana Editores, 2011.

Normativa nacional e internacional

Brasil. *Lei Geral de Proteção de Dados Pessoais*. Diário Oficial da União, 14 de agosto de 2018.

———. *Marco Civil da Internet*. Diário Oficial da União, 23 de abril de 2014.

———. *Ley Carolina Dieckmann*. Diário Oficial da União, 3 de diciembre de 2012.

———. *Projeto de Lei nº 2338*. Diário Oficial da União, 3 de mayo de 2023.

Colombia. *Ley Estatutaria para la Protección de Datos Personales*. Diario Oficial de la República, 18 de octubre de 2012.

———. *Ley 1273*. Diario Oficial de la República, 5 de enero de 2009.

———. *Ley 2502*. Diario Oficial de la República, 28 de julio de 2025.

Ecuador. *Constitución de la República del Ecuador*. Registro Oficial 449, Suplemento, 20 de octubre de 2008.

———. *Código Civil*. Registro Oficial 46, Suplemento, 24 de junio de 2005

———. *Código de la Niñez y Adolescencia*. Registro Oficial 737, Suplemento, 03 de enero de 2003.

———. *Código Orgánico Administrativo*. Registro Oficial 31, Suplemento, 7 de julio de 2017.

———. *Código Orgánico de la Economía Social de los Conocimientos*, Registro Oficial, Suplemento 889, 9 de diciembre de 2016.

———. *Código Orgánico Integral Penal COIP*. Registro Oficial 180, Suplemento, 10 de agosto de 2014.

———. *Norma Técnica del Servicio de Atención y Protección Emergentes del MIES*. Registro Oficial 694, Suplemento Cuarto, 29 de noviembre de 2024.

———. *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*. Registro Oficial 52, Suplemento, 22 de octubre de 2009.

———. *Ley Orgánica de Protección de Datos Personales*. Registro Oficial 459, 18 de octubre de 2012.

———. *Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación*. Registro Oficial 401, Suplemento, 21 de octubre de 2023.

———. *Protocolo para la atención de llamadas de emergencia relacionadas con violencia de género e intrafamiliar recibidas por el ECU-911*. Registro Oficial 411, Suplemento, 05 de octubre de 2023.

México. *Guía para el ejercicio de los derechos ARCO*. Sitio web institucional INAI. 6 de enero de 2012.

———. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Diario Oficial de la Federación. 21 de marzo de 2025

ONU Asamblea General. *La Declaración Universal de los Derechos Humanos*. 10 de diciembre de 1948. A/RES/217/3.

———. *Pacto Internacional de Derechos Civiles y Políticos*. 16 de diciembre de 1966. A/RES/21/2200 A.

UE Parlamento y Consejo Europeo. *Digital Services Act.* 19 de octubre de 2022. A/RES/2022/2065.

———. *Reglamento de la Inteligencia Artificial (AI Act)*. 13 de junio de 2024. A/RES/2024/1689.

———. *Reglamento General de Proteccion de Datos de la Unión Europea*. 27 de abril de 2016. A/RES/2016/679.

———. *Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia*, 23 de noviembre de 2001, A/RES/132/224.

UNESCO Conferencia General. *Recomendación sobre la ética de la inteligencia artificial*. 23 de noviembre de 2021. A/RES/41/36.

Jurisprudencia

Ecuador Corte Constitucional. "Sentencia". *Juicio n.°: 1497-20-JP/21*, 21 de diciembre de 2021.

———. "Sentencia". *Juicio n.º: 2539-18-EP/24*, 01 de agosto de 2024.

———. "Sentencia". *Juicio n.º: 2063-17-EP/22*, 27 de julio de 2022.

———. "Sentencia". *Juicio n.º: 11-18-CN/19*, 19 de junio de 2019.

———. "Sentencia". *Juicio n.º: 2064-14-EP*/21, 27 de enero de 2021.

Anexos

Anexo 1: Entrevista a Sofía León (seudónimo)

1.- Buenas tardes coméntame, ¿Cómo te llamas, cuantos años tienes, tú estudias, qué cosas te gusta hacer en tu tiempo libre y cómo fue que empezaste a usar nuevas tecnologías como la inteligencia artificial?

Me llamo Sofía León (seudónimo), tengo 17 años y vivo con mi mami en Los Chillos. Si estudio, estoy en el último año del cole, en mi tiempo libre me gusta leer, salir con mis amigas y jugar básquet, que me ayuda a soltar el estrés y despejarme un poco. Conocí la inteligencia artificial en pandemia, cuando usaba ChatGPT para hacer tareas o buscar respuestas cuando tenía dudas, me pareció súper útil, aunque también me di cuenta de que hay que tener cuidado con cómo se usa. Hace dos años viví algo que me afectó a mí y a mis compañeras en el cole.

2.- Sofía, ¿Puedes contarnos que fue lo que paso hace dos años que marcó tu vida estudiantil?

Yo fui víctima de un video porno que hicieron mis propios compañeros, yo no sabía que se podía hacer algo así… usaron inteligencia artificial para poner mi cara en un video sexual. Una amiga me lo mostró y sí, era mi cara, pero no era yo. ¡Me quedé en shock! No entendía cómo podía estar pasando eso, el video lo habían publicado en TikTok, y eso me dio terror, porque cualquiera podía verlo. Le conté al tutor y él nos escuchó y dijo que nos iba a apoyar, pero al final no hizo nada. Me sentí sola y estaba triste, yo me puse a llorar, no sabía qué hacer. Apenas llegué a la casa me metí directo a mi cuarto, no quería salir ni ver a nadie. Me sentía avergonzada y con miedo de que mi familia viera el video y pensara que era yo. No quería dar explicaciones ni hablar de nada… pasaron unos días y, aunque me costó, me decidí y le conté a mi mami. Ella me abrazó, me dijo que esté tranquila, que iba a estar conmigo y que me iba a ayudar. Eso me calmó y me hizo sentir más tranquila.

3.- ¿Cómo te hizo sentir saber que, a pesar de todo lo que pasó, nadie decía ni hacía nada?

Yo me sentía cada vez más triste, hubo compañeros que nos apoyaron, pero también mucha gente que nos miraba feo, que hablaba mal de nosotras, decían cosas horribles como que éramos fáciles o que queríamos llamar la atención, como si fuera

culpa nuestra. Eso era doloroso porque no sabían nada y aun así nos juzgaban. Pasaban los días y nadie hacía ni decía nada. Me daba miedo entrar al aula, cruzarme con ciertas personas, escuchar sus risas o sus comentarios, dejé de hablar con algunos amigos, a veces ni comía, solo quería llegar a casa y encerrarme en mi cuarto. Y eso fue lo que más dolió, que todo quedara así, como si nunca hubiera pasado, como si nosotras tuviéramos que seguir como si nada, cargando con algo que no hicimos.

A veces pensaba que todo habría pasado más rápido si solo hubiesen sido unas fotos que se borraban, pero no fue así. Los profes y la madre superiora no hicieron nada, nadie nos apoyó. Mi familia sí estuvo conmigo, sobre todo mi mami, aunque verla tan triste me dolía. Decidí cambiarme de colegio; al principio fue duro, me sentía aislada y extrañaba a mis amigas, pero también sentía alivio de no enfrentar esas miradas. Luego supe que las otras chicas siguieron con sus vidas y ya casi nadie hablaba del tema. Ahora es normal ver tu cara en otro cuerpo como si fuera un meme. La gente lo comparte y se ríe, pero cuando te pasa, lo ves diferente: sí afecta, te hace sentir que pierdes el control sobre tu vida y tu cuerpo. Por suerte logré salir de eso, aunque fue difícil. Me costó volver a confiar y sentirme segura. A veces todavía me da miedo que vuelva a pasar

4. Finalmente, ¿hay algo que te gustaría decirle a alguien que esté pasando por una situación parecida a la que tú viviste?

Si alguien está pasando por algo parecido a lo que yo viví, lo primero que le diría es que no está sola. Aunque en el momento todo se sienta que nadie te cree o te defiende, hay personas que sí te van a escuchar y te van a creer de verdad. A mí me costó confiar otra vez, volver a sentirme segura, pero poco a poco lo fui logrando. Si te pasa algo así, habla con alguien que te quiera, que no te juzgue, no te guardes todo, a veces solo necesitamos que alguien nos abrace y nos diga que lo que sentimos está bien, que no estamos exagerando. Y también diría que lo que pasa en internet sí duele, que no es un chiste, que cuando ponen tu cara en algo que no hiciste, te pueden llegar a afectar, pero que no dejen que les hagan sentir menos, porque que valen muchísimo.

Anexo 2: Entrevista a María León (seudónimo)

1. ¿Podría compartirnos quién es usted desde su experiencia y qué le impulsó a formar parte de esta entrevista?

Soy María León (seudónimo), tengo 38 años, soy madre de Sofía e ingeniera. Decidí participar en esta entrevista porque considero que es un espacio de reflexión valioso. Agradezco que se aborde un tema tan sensible en tu investigación de posgrado, que no solo aporta a tu formación, sino que marca un precedente para futuros registros. Cuando esto ocurrió con mi hija, era una problemática poco visibilizada, hoy en día con el avance tecnológico, los casos se multiplican y conlleva profundas repercusiones familiares y emocionales. Espero que este espacio contribuya a abrir caminos hacia políticas públicas que ayuden a controlar una situación desbordante.

2. ¿Cómo se enteró de que su hija había sido víctima en este caso de esta creación digital que al día de hoy sabemos que se trata de un *deepfake* pornográfico?

Se supo que estudiantes de segundo de bachillerato habían creado y difundido ese contenido, afectando a varias niñas. La institución encubrió el hecho, silenció a los padres e incluso me apagaron el micrófono cuando intenté hablar, formamos un grupo de WhatsApp, pero la información era confusa. Me enteré por otra madre que el DECE tenía sus celulares como evidencia, una doctora de una fundación nos ayudó a visibilizar el caso en medios, lo que generó presión y manifestaciones estudiantiles, la institución respondió acusando a los padres de desprestigiarla. Aunque el Ministerio activó el denunció a la Fiscalía, los padres no se unieron, yo encabecé la denuncia, pero decidí no continuar sola, prometieron atención emocional para las niñas, pero no se cumplió y los chicos fueron retirado del colegio. Fiscalía nos dijo que era un proceso largo, sin registros ni leyes claras, la justicia fue sin acompañamiento real, el tiempo agravó la situación, y hoy en día este tipo de situaciones son comunes.

3. ¿Qué impacto tuvo este evento en su vida, en la de su hija y en su familia?

Mi hija no comprendía lo que estaba pasando, le expliqué que, aunque no fuera su cuerpo, su rostro podía ser visto por cualquier pedófilo, y eso no estaba bien. La situación se volvió más difícil, mi hija se entristeció profundamente, sobre todo por la revictimización que sufrió en el colegio, aunque hubo protestas internas en apoyo a las niñas, también hubo chicos que no entendieron la gravedad del hecho. Esa falta de empatía y de consecuencias fue lo más doloroso, todo quedó en el olvido, no hubo sanciones, ni campañas informativas sobre los riesgos de las redes sociales y la

inteligencia artificial. La impunidad fue total, a pesar de ello, salimos fortalecidas, gracias al diálogo, aunque no recibimos ayuda psicológica de nadie, fue un proceso que atravesamos juntas.

4. ¿Qué afectación emocional pudo percibir en ese momento?

Fueron días sin dormir, de profunda tristeza y de tener que aparentar fortaleza donde no había. Lloré muchas noches por la situación, porque sentirse sola en una comunidad educativa y ver cómo se vulneran los derechos, da mucho que pensar. Aunque la institución es reconocida académicamente en el Valle de los Chillos, no protegió a sus estudiantes ni siguió protocolos, lo que generó desesperación y angustia. Ser silenciada y etiquetada como parte del "grupo de los problemáticos" fue muy duro, incluso más que la violencia digital. Lo más doloroso fue ver cómo la sociedad cierra las puertas frente a una verdad completa. Me sentía devastada, pero cuando los medios presionaron y el colegio finalmente puso la denuncia, decidí que hasta ahí llegaba mi lucha.

5. ¿Se podría decir que la presión mediática ayudó para que se dé una visibilización de la problemática?

Los medios de comunicación fueron clave para que el colegio actuara; sin ellos, no habría pasado nada. Gracias a esa presión se presentó la denuncia, aunque la Fiscalía no dio seguimiento: solo hubo una reunión breve con padres, sin hablar con las niñas ni mostrar evidencia. Todo quedó guardado por la institución. Entiendo que dos jóvenes descargaron fotos de redes sociales de niñas seleccionadas, muchas bastoneras o cheerleaders, y usaron sus rostros, no sabemos qué hicieron con las imágenes. Es casi imposible rastrearlas sin apoyo técnico, yo decidí no continuar con una denuncia particular. El uso del término "presunto" fue desgastante, denuncié ante la institución para que no se repita y dejé el proceso en sus manos, por mi salud mental.

6. ¿Cómo percibió la respuesta de las autoridades y cuál sería la reflexión final podría compartirnos de esta experiencia?

La institución no hizo absolutamente nada; todo siguió como si nada hubiera pasado. La Fiscalía solo ofreció una reunión virtual de media hora para padres, sin acercamiento real a las estudiantes. El Ministerio de Educación acudió tras la presión mediática, pero solo hizo preguntas a las chicas, sin seguimiento. Desde mi perspectiva, el sistema es precario, no hay leyes que sancionen este tipo de hechos, ni campañas escolares que concienticen el manejo responsable de la imagen de las niñas, que son las más afectadas. Para mí, esto sí es un delito, aunque no lo consideren así, a eso se sumó la negligencia institucional y la falta de empatía hacia las niñas. En cuanto al apoyo

psicológico, el colegio solo ofreció una charla, pero yo necesitaba un certificado que demostrara que mi hija estaba bien.

A pesar de lo duro cuando hay una razón para alzar la voz, hay que hacerlo con fortaleza, descubrí que esa es una de mis mayores virtudes. Los mecanismos de investigación permiten visibilizar estas realidades y reformar las leyes. Hoy es difícil controlar la imagen; nadie está exento de la violencia, por eso debemos cuidar lo que subimos y denunciar cuando se vulnera nuestra dignidad. Hay gente malintencionada, pero también tecnología que puede usarse bien, lo importante es hacer lo que esté en nuestras manos y seguir adelante.

Anexo 3: Entrevista a Simón Rivas (seudónimo)

1. ¿Podría contarnos un poco sobre usted, sobre su vida?

Mi nombre es Simón Rivas (seudónimo), estoy por cumplir 45 años, soy abogado de profesión, con experiencia en el ámbito político. Actualmente me dedico casi por completo a la docencia, con más de una década como profesor de pregrado y posgrado. He ocupado cargos de dirección académica y actualmente coordino programas de maestría. Estoy casado y tengo dos hijos, actualmente soy secretario nacional en mi partido político y he participado en la conformación de listas electorales provinciales y nacionales.

2. ¿Cuál es su opinión acerca de la inteligencia artificial y cuál ha sido su acercamiento de manera personal a este tipo de tecnología?

La inteligencia artificial es una herramienta instrumental, no es buena ni mala, pero su impacto depende del uso ético y responsable que le dé cada individuo. La IA puede facilitar procesos o causar daño, la responsabilidad recae en quien la manipula. Aunque me capacito constantemente en herramientas digitales, incluida la inteligencia artificial, para mejorar mi labor docente, estas herramientas han sido útiles, especialmente en la coordinación de posgrados. Sin embargo, mi trayectoria como abogado, mi participación política y mi rol académico han generado amistades y enemigos, la política se vive como agresión al disidente, y en la academia, exigir excelencia genera resistencia.

Al asumir la dirección de la carrera de pregrado en la Universidad, fui convocado a una reunión urgente con autoridades, me mostraron siete fotografías algunas eran capturas reales de zoom, otras manipuladas. Las imágenes se enviaban por WhatsApp. Aunque parecían reales, sabía que no eran mías, el gerente sugirió que podrían haber sido generadas con inteligencia artificial. El número provenía de Burkina Facio, lo que inquietó a las autoridades por posible chantaje. Las imágenes no llegaron, solo recibí un mensaje extraño que bloqueé, ya había denunciado el hecho. La situación generó sospechas, afectó mi trayectoria justo cuando podía ser nombrado decano, y se agravó por el vínculo de la universidad con el Opus Dei.

3. ¿Sintió en algún momento falta de protección por parte de la universidad, algún tipo de discriminación o que las fotos fueron tomadas como reales?

Sentí que las autoridades universitarias asumieron que las imágenes manipuladas podían ser reales, lo que afectó mi imagen y frustró mi ascenso al decanato. Aunque se corrigió tras la denuncia, la relación institucional se deterioró y terminé saliendo de la

universidad. Me pidieron llamar a mi esposa para mostrarle las fotos; ella confirmó que no era yo, y eso me dio fuerza para denunciar. Tenía desconfianza con el vicerrector académico, y me pareció extraño que las imágenes solo llegaran a la universidad. Al día siguiente, presenté la denuncia ante la Fiscalía. Ese mismo día, las fotos llegaron al correo del Instituto Ecuatoriano de Derecho Tributario, donde iba a moderar un evento. Un policía dijo que probablemente provenían de la cárcel de Latacunga, como parte de un sistema de extorsión.

Tras presentar la denuncia, la Universidad abrió un expediente ético en mi contra, pero lo cerraron al recibir el informe policial. Aun así, la relación se deterioró y un año después salí de la institución. También hubo tensiones en el Instituto Ecuatoriano de Derecho Tributario, donde presidí antes. Me comentaron que el presidente actual había traído las fotos, lo que me hizo pensar en rencillas internas. La policía investigó correos vinculados al caso, pero fueron borrados. Me dijeron que el origen era local, posiblemente desde la cárcel de Latacunga, y que alguien cercano buscaba dañar mi imagen. Cerré mis redes por el impacto del mensaje, que incluía una acusación con una “niña de 12 años”, algo grave en una universidad vinculada al Opus Dei. Con el tiempo, perdí la vergüenza de hablar del tema. Mi esposa, ingeniera en sistemas, revisó las fotos y notó que estaban manipuladas. Aunque la denuncia sigue archivada, nunca se identificó al responsable.

Anexo 4: Entrevista a Luis Enriquez

1. **Buenos días, coménteme ¿Quién es y a qué se dedica?**

Soy Luis Enríquez, docente e investigador en la Universidad Andina Simón Bolívar. Me especializo en derecho digital y protección de datos, campos que he profundizado a través de una formación internacional, soy Doctor en Derecho por la Université de Lille, LL.M. en Tecnologías de la Información por la Leibniz Universität Hannover y Magíster en Derecho Económico Internacional por la propia Andina, donde actualmente dirijo el Máster en Derecho Digital de la Economía.

2. ¿Qué es la inteligencia artificial y cómo ha evolucionado a lo largo del tiempo hasta permitir la creación de los *deepfakes*?

La IA surge en el siglo XX como una ciencia orientada a que las máquinas realicen tareas propias de la inteligencia humana. Con el tiempo, el concepto se ha vuelto más abstracto, y algunos lo comparan con la búsqueda de una inteligencia alienígena. Es clave distinguir entre la IA como idea general y sus metodologías, especialmente el aprendizaje automático, que entrena sistemas para actuar con autonomía, ya sea mediante modelos supervisados o no supervisados, como los usados en *deepfakes* con redes generativas adversarias (GANGs). Dentro del aprendizaje profundo destacan las redes neuronales, base de la IA generativa. En el reglamento europeo evita definir la IA, reflejando la dificultad de precisar un concepto que aún se mide contra una idea idealizada de inteligencia humana. El *deepfake* es una técnica basada en aprendizaje profundo que genera contenidos falsos mediante algoritmos predictivos y modelos no supervisados. Utiliza GANGs para imitar rostros, voces o datos biométricos, insertándolos en contextos distintos al original. Aunque se aplica principalmente en imágenes y videos, también puede manipular audio y otros formatos sensibles.

3. ¿Qué factores tecnológicos han facilitado la proliferación de los deep fake pornográficos o su creación y qué derechos de las personas está afectando este tipo de contenidos digitales?

El *deepfake* es una técnica algorítmica que permite manipular imágenes, audios y videos para crear contenidos falsos. Aunque empezó como parodia o entretenimiento, hoy se usa para vulnerar la seguridad digital, suplantar identidades y cometer delitos como fraude, chantaje o violencia sexual digital. Cualquier persona puede generar estos contenidos sin conocimientos técnicos, lo que agrava el riesgo jurídico y ético. En el ámbito pornográfico, se insertan rostros de personas inocentes en escenas sexuales falsas,

afectando su honra y privacidad. Aunque el Reglamento Europeo de IA reconoce los *deepfakes*, no existe una tipificación penal directa. La falta de formación tecnológica en el gremio jurídico impide respuestas eficaces, la única estrategia viable es la detección automatizada en tiempo real, especialmente en contextos pornográficos. En Ecuador y Latinoamérica, los debates legislativos carecen de expertos técnicos, lo que genera un desfase entre regulación y realidad digital. La solución no está en garantizar desde el derecho, sino en adoptar una protección proactiva mediante sistemas de detección basados en modelos probabilísticos como Naive Bayes, regresión o Random Forest, la IA se basa en gestión de riesgos, no en certezas jurídicas.

4. ¿Cómo formar abogados capaces de legislar sobre inteligencia artificial y riesgos digitales?

En Ecuador, las mesas de discusión sobre leyes carecen de expertos en tecnología, predominan abogados que desconocen el funcionamiento real de la inteligencia artificial. Esto dificulta una regulación adecuada, la solución no está en prohibir, sino en adoptar una protección proactiva, con sistemas que detecten *deepfakes* y eviten replicar contenidos ilícitos y modelos de clasificación como Naive Bayes, regresión o Random Forest, pero siempre existe un riesgo residual. La IA se basa en gestión de riesgos, no en certezas jurídicas, por lo que términos como "garantizar" resultan obsoletos. Es urgente que los abogados estudien estadística, machine learning y lógica algorítmica para convertirse en ingenieros jurídicos. El marco regulatorio ecuatoriano es limitado en temas tecnológicos, la mayoría de asambleístas tienen escasa cultura digital, lo que impide enfrentar los desafíos actuales.

5. ¿Cómo puede Ecuador regular los efectos nocivos de la inteligencia artificial sin frenar la innovación tecnológica ni vulnerar libertades?

En Ecuador la regulación de inteligencia artificial, las universidades están rezagadas y las mesas legislativas carecen de expertos tecnológicos; predominan abogados sin formación técnica. La regulación debe centrarse en la protección de derechos, no en prohibir metodologías ni tecnologías como *deepfakes*. El enfoque debe estar en el bien jurídico afectado, no en la tecnología, la gestión del riesgo es clave no se trata de atacar la herramienta, sino el uso nocivo que vulnera derechos y libertades. El *soft law* no es suficiente; sin sanción, la ética queda como placebo. Se necesita *hard law* bien enfocada, que abarque lo penal, administrativo, constitucional y civil. La regulación debe ser proactiva y reactiva, con mecanismos para detectar y prevenir delitos digitales. La misma tecnología puede ayudar a mapear riesgos y proteger a la ciudadanía.

Anexo 5: Entrevista a Cristian Masapanta

1. **Buenas tardes, coménteme ¿Quién es usted y a qué se dedica?**

Mi nombre es Cristian Masapanta Gallegos, mi formación académica está vinculada al derecho constitucional, tengo una especialización superior en justicia constitucional, una maestría internacional en derecho constitucional y un doctorado enfocado en interpretación constitucional y garantías jurisdiccionales. Soy docente a tiempo completo en la Universidad Andina Simón Bolívar, donde coordino varios programas de posgrado, además de ejercer como docente en otras instituciones de educación superior.

2. ¿Desde su perspectiva constitucional cómo define el habeas data y cuál es el alcance actual en la protección de los derechos fundamentales en entornos digitales?

El habeas data suele pensarse erróneamente como una garantía jurisdiccional, cuando en realidad, desde la vía estatal ecuatoriana, se configura como un verdadero derecho constitucional, la Constitución y los instrumentos internacionales de derechos fundamentales garantizan no solo la existencia de datos personales, sino también el acceso, modificación, rectificación y conocimiento de su uso. En el ámbito doctrinario existe un debate constante, ¿es un derecho o una garantía para proteger derechos constitucionales? Esta figura tiene una doble dimensión, proteger datos personales y vincular a los bienes de una persona. Además, ha evolucionado hacia una garantía de conocimiento que permite un análisis profundo sobre su tutela, superando la autodeterminación informativa inicial. Ya no se limita a proteger el derecho subjetivo a la información personal, sino que se conecta con otros derechos constitucionales como el honor, el nombre, la dignidad y la intimidad, que pueden verse afectados por el mal uso de los datos.

3. ¿Cree usted que podría evolucionar, como usted mismo lo menciona, existe esta vulneración a derechos conexos a una figura que proteja no solo los datos personales, sino también a la imagen digital como proyección simbólica del cuerpo y la dignidad de la persona?

El derecho, como construcción social, debe adaptarse a las necesidades emergentes. El constituyente no puede prever el futuro, por lo que las normas deben ajustarse a la realidad cambiante. En Ecuador se incorporó el habeas data como garantía de fondo y conocimiento. Esta figura jurídica debe evolucionar frente a desafíos como las nuevas tecnologías, que pueden afectar derechos como la dignidad e intimidad. Aunque

no se puede reformar la Constitución constantemente, sí es posible generar desarrollo jurisprudencial desde la Corte Constitucional. Un ejemplo es la Sentencia Nº 2064-14-EP/21 de Corte Constitucional, que prohíbe publicar fotos íntimas y reconoce la afectación a derechos conexos, evidenciando la necesidad de proteger datos personales, tanto individuales como colectivos.

4. ¿Qué tensiones usted ha identificado entre el habeas data y la libertad de expresión que también es un derecho importante en plataformas digitales y frente a la circulación de contenidos falsificados?

La tensión entre intimidad y libertad de expresión en entornos digitales exige analizar la expectativa razonable de privacidad, que varía según la plataforma. No toda difusión de datos personales vulnera la intimidad; debe contextualizarse. El *habeas data* puede resignificarse como herramienta de reparación simbólica y material ante violencia digital. Desde 2008, las garantías jurisdiccionales se dividen en cautelares y de conocimiento; esta última permite evaluar el daño, escuchar a la víctima y establecer medidas eficaces, la reparación debe ser integral y adaptada al grado de afectación.

5. ¿Qué reformas según su criterio permitirían que el habeas data responda a los desafíos de IA generativa mediante la cual se está generando el contenido digital y especialmente ante la violencia simbólica y la afectación de la dignidad humana?

No me identifico con el punitivismo y considero que el derecho penal debe ser de última ratio. Aunque se plantean reformas al COIP para incorporar nuevos tipos penales frente a realidades tecnológicas emergentes, como la inteligencia artificial, creo que la solución no debe ser únicamente normativa. Es fundamental trabajar desde la prevención, el diálogo y la construcción ética. Las empresas que gestionan estas tecnologías deben asumir protocolos éticos, identificar riesgos y garantizar transparencia: informar al usuario sobre el uso de sus datos y construir entornos digitales equitativos. Hoy enfrentamos un avance tecnológico arrollador, y como advierte Zaffaroni con su metáfora del río de aguas turbias, si no se construyen diques éticos, se arrasará con todo. Estos diques deben proteger los derechos fundamentales.

Anexo 6. Entrevista a Santiago Acurio del Pino

1. **Buenas tardes, coméntenos ¿Quién es usted y a qué se dedica?**

Soy abogado y doctor en Jurisprudencia por la Pontificia Universidad Católica del Ecuador. Me especialicé en Derecho Penal en la Universidad Andina Simón Bolívar y cursé dos maestrías: una en Tecnologías para la Gestión y Práctica Docente en la PUCE, y otra en Derecho Digital, Transformación Digital y Economía Digital en la UDLA. Actualmente me dedico a la docencia universitaria, la investigación en derecho penal informático y ciberseguridad, y colaboro como instructor internacional en cibercrimen para la OEA.

2. ¿Debe considerarse la creación y difusión de *deepfakes* pornográficos como una forma de violencia sexual digital, aun cuando no exista contacto físico o participación directa de la víctima?

Existen contenidos digitales como los deepfakes basados en video, audio, imágenes generadas por IA, que deben considerarse violencia digital, especialmente contra mujeres. El caso de Taylor Swift evidencia cómo la IA genera contenido sexual no consentido, se viraliza en plataformas como Telegram, X y TikTok. También hay riesgo para niñas, niños y adolescentes, como muestra Europol, al facilitar nuevas formas de explotación sin víctimas físicas directas, aprovechando vacíos normativos. El COIP sanciona con 13 a 16 años la producción de material visual, real o simulado, de menores en actividad sexual. Pero los deepfakes son representaciones visuales realistas generadas por IA, especialmente mediante redes generativas antagónicas (GANs). El art. 22 del COIP exige que la conducta lesione un bien jurídico protegido, como la dignidad humana, la pornografía infantil es un delito contra la dignidad, no de carácter sexual.

3. ¿Qué bienes jurídicos se ven comprometidos a través de los *deepfakes* pornográficos y cómo debería el derecho penal protegerlos frente a estas nuevas agresiones?

El deepfake pornográfico constituye un delito pluriofensivo que afecta la intimidad, imagen, privacidad, datos personales y, sobre todo, la dignidad humana, entendida desde una visión kantiana como valor incondicional y fundamento de los derechos fundamentales. Aunque no está tipificado en el COIP, puede considerarse un delito de resultado, peligro abstracto o concreto, según el daño configurado, como en el grooming o el pánico financiero. La creación y difusión de contenido falso mediante IA

con intención de causar daño patrimonial, reputacional o emocional exige revisar el tipo penal, considerando la lesión efectiva y el bien jurídico protegido.

4. **¿Qué criterios debería considerar la política criminal para sancionar estos delitos sin incurrir en una sobrerregulación que afecte la libertad de expresión o el uso legítimo de tecnologías creativas? Es decir, cómo regular sin inhibir la innovación**.

La política criminal debe basarse en el principio de responsabilidad respetando el libre desarrollo de la personalidad establecido en la Constitucion, limitado por los derechos de los demás. Ante su lesión, el derecho actúa como control social y formal a través de las leyes o desformalizado a través de la educación y la ética. Prevalece el principio de mínima intervención penal y subsidiariedad, solo se recurre al derecho penal cuando no hay otra vía. Esto evita su expansión simbólica o punitiva, en un Estado garantista, el debido proceso limita el poder de castigar, la política criminal debe estar anclada en la Constitución y el COIP, orientada a la prevención general, rehabilitación del infractor y reparación integral de la víctima, en línea con el funcionalismo moderado de Roxin.

Anexo 7: Entrevista a Ibán García del Blanco

1. **Buenas tardes, coménteme ¿Quién es usted y a qué se dedica?**

Soy Ibán García del Blanco, abogado de formación y eurodiputado por el Partido Socialista Obrero Español desde 2019. Mi trayectoria política ha estado marcada por el compromiso con la cultura, la innovación y los derechos digitales. He presidido instituciones como Acción Cultural Española y la Fundación Pablo Iglesias, y actualmente trabajo en el Parlamento Europeo impulsando marcos normativos que regulen la inteligencia artificial y protejan los derechos fundamentales.

2. ¿Cómo se aborda jurídicamente el uso de la IA para generar contenido, ese tipo de contenido no consentido como son los *deepfakes* pornográficos, y existe alguna categoría específica de riesgo en la normativa para estos casos?

La inteligencia artificial, por sus características particulares, potencia y capacidad de generar daño, requiere una norma específica que establezca categorías de riesgo. En el caso de la inteligencia artificial generativa, se añade un capítulo de prevención centrado en normas de transparencia, como la obligación de etiquetar los contenidos creados con IA. Si su uso afecta derechos fundamentales, deben aplicarse también normas sobre riesgos, incluyendo usos prohibidos o de alto riesgo. Sin embargo, esto no implica que el resto del derecho pierda vigencia, la IA es una herramienta más, y el derecho debe responder igual si se vulnera la dignidad o la imagen personal, sea con IA o con medios tradicionales.

3. ¿Qué mecanismos de protección contempla la ley para las víctimas de manipulación digital íntima y especialmente en contextos de violencia simbólica se prevé algún tipo de reparación o acceso a una justicia transnacional?

La Ley de Inteligencia Artificial de la UE no agota el tratamiento jurídico de los posibles ilícitos; el derecho privado y público siguen vigentes. Sin embargo, su incumplimiento sí conlleva sanciones proporcionales al daño y a la capacidad del infractor, pudiendo alcanzar hasta el 7% de la facturación mundial en casos graves o reiterados. Además, los modelos generativos más potentes, considerados de riesgo sistémico, deben cumplir obligaciones previas a su comercialización, como medidas de transparencia y eliminación de sesgos. La ley tiene carácter exhaustivo respecto a todos los actores del tráfico jurídico, desde desarrolladores hasta usuarios, pudiendo derivar incluso en responsabilidades personales. En cuanto a la supervisión, la Oficina Europea de Inteligencia Artificial ejerce competencias específicas sobre modelos generativos,

incluyendo el registro y las reclamaciones. El resto de la implementación de la ley se realiza a nivel nacional, con organismos designados por cada Estado según el ámbito de aplicación.

4. ¿Considera que la legislación europea puede inspirar marcos normativos por ejemplo en América Latina, específicamente en el Ecuador en donde hay un vacío legal frente a esta violencia digital y qué rol podrían tener los tratados internacionales en esta materia?

La experiencia europea en la regulación de la inteligencia artificial, con sus aciertos y errores, debería ser aprovechada por el resto del mundo para establecer marcos normativos propios, adaptados a cada país o región. Aunque no se trata de copiar la normativa europea, su enfoque en la protección de derechos fundamentales y valores colectivos es acertado y escalable. Algunos países latinoamericanos, como Brasil, ya han adoptado modelos similares. En este contexto, se destaca la importancia de una integración regional en América Latina para evitar la competencia normativa a la baja y enfrentar con mayor fuerza la presión de grandes desarrolladores tecnológicos. La Unión Europea, como bloque de 27 estados soberanos, tiene una capacidad regulatoria sólida que debería inspirar a la región.

5. ¿Es necesario un enfoque ético y educativo que promueva la dignidad digital y el respeto a la intimidad en entornos virtuales y hasta dónde sería necesario su enfoque ético y comenzaría a validarse la regulación?

Es absolutamente necesario tomar conciencia de que el ejercicio de la ciudadanía, hoy y aún más en el futuro, dependerá de nuestra capacidad para comprender el entorno digital y sus herramientas. Esto afecta desde el ejercicio de derechos frente a administraciones o empresas, hasta la integración laboral, la formación y la competitividad. Por ello, más allá de la regulación institucional, la formación y la ilustración digital son esenciales para una ciudadanía de calidad. Frente a fenómenos como los *deepfakes* o contenidos pornográficos falsos generados con inteligencia artificial, la ley penal puede ser dura, pero la principal forma de combatirlos es el conocimiento: ser cautelosos con nuestros datos, conscientes de los riesgos y de que ciertas acciones están mal y pueden ser sancionadas, la labor es urgente y el tiempo apremia.