Revista científica Sociedad & Tecnología

ISSN: 2773-7349

fecha de presentación: 20/07/2025, fecha de aceptación: 15/08/2025, fecha de publicación: 10/09/2025

Lilia Margarita Taco-Sánchez
E-mail: Itaco4@indoamerica.edu.ec magytaco@gmail.com
Orcid: https://orcid.org/0009-0000-7536-5600

Francisco David Villacis-Mogrovejo
E-mail: franciscovillacis@uti.edu.ec,
Orcid: https://orcid.org/0009-0008-7302-1634

Carrera de Derecho, Universidad Tecnológica Indoamérica. Ambato, Ecuador

Cita sugerida (APA, séptima edición)

Taco-Sanchez, L. M., & Villacis-Mogrovejo, F. D. (2025). Delitos Digitales de contenido íntimo generado mediante inteligencia artificial: Análisis de la necesidad de una regulación especial en Ecuador. *Revista Sociedad & Tecnología*, 8(S2), 607-622. DOI: https://doi.org/10.51247/st.v8iS2.68.

==== o ====

Delitos Digitales de contenido íntimo generado mediante inteligencia artificial: análisis de la necesidad de una regulación especial en Ecuador

RESUMEN

El presente artículo tuvo como objetivo analizar la necesidad de incorporar un tipo penal específico en el Código Orgánico Integral Penal (COIP) de Ecuador para sancionar la creación y difusión de contenido íntimo no consentido generado mediante inteligencia artificial (deepfakes), debido al vacío normativo que actualmente impide una protección adecuada de las víctimas. La metodología empleada fue de corte cualitativo, utilizando los métodos de revisión bibliográfica, análisis jurídico y derecho comparado, especialmente con el caso español. Entre los principales resultados se evidencia que el 96 % de los deepfakes detectados en Internet son pornográficos y afectan principalmente a mujeres; además, más del 80 % de los operadores de justicia ecuatorianos consideran que la legislación actual es insuficiente para enfrentar este tipo de ciberdelitos. Como conclusión, se destaca la urgencia de reformar el COIP mediante la creación de un tipo penal autónomo que contemple la especificidad técnica y social de los deepfakes sexuales no consentidos, así como la necesidad de fortalecer las capacidades institucionales y judiciales, promoviendo un enfoque integral que combine sanción penal, prevención, reparación a las víctimas y educación digital.

Palabras Clave: Contenido íntimo no consentido, Deepfakes, Inteligencia artificial, Regulación penal, Violencia digital.

==== O ====

Digital Crimes involving intimate content generated by artificial intelligence: analysis of the need for special regulation in Ecuador.

ABSTRACT

This article aims to analyze the need to incorporate a specific criminal offense into Ecuador's Comprehensive Organic Criminal Code (COIP) to sanction the creation and dissemination of

non-consensual intimate content generated through artificial intelligence (deepfakes), due to the current legal vacuum that prevents adequate protection for victims. The methodology used was qualitative, employing literature review, legal analysis, and comparative law methods, particularly with the Spanish case. Among the main findings, it is evident that 96% of deepfakes detected on the Internet are pornographic and primarily affect women; additionally, over 80% of Ecuadorian justice system operators believe that current legislation is insufficient to address this type of cybercrime. In conclusion, the article highlights the urgent need to reform the COIP by creating an autonomous criminal offense that reflects the technical and social specificities of non-consensual sexual deepfakes, as well as the need to strengthen institutional and judicial capacities, promoting a comprehensive approach that combines criminal sanctions, prevention, victim reparation, and digital education.

Keywords: Non-consensual intimate content, Deepfakes, Artificial intelligence, Criminal regulation, Digital violence.

==== O ====

Crimes Digitais envolvendo conteúdo íntimo gerado por inteligência artificial: análise da necessidade de regulamentação especial no Equador

RESUMO

Este artigo teve como objetivo analisar a necessidade de incorporar um tipo penal específico ao Código Penal Orgânico Integral (COIP) do Equador para punir a criação e a disseminação de conteúdo íntimo não consensual gerado por inteligência artificial (deepfakes), devido à lacuna regulatória que atualmente impede a proteção adequada das vítimas. A metodologia empregada foi qualitativa, utilizando revisão bibliográfica, análise jurídica e direito comparado, especialmente com o caso espanhol. Entre os principais resultados, evidencia-se que 96% dos deepfakes detectados na internet são pornográficos e afetam principalmente mulheres; além disso, mais de 80% dos funcionários da justiça equatoriana consideram a legislação atual insuficiente para lidar com esse tipo de crime cibernético. Concluindo, destacamos a necessidade urgente de reformar o Código de Infrações Penais (COIP), criando uma infração penal independente que aborde a especificidade técnica e social dos deepfakes sexuais não consensuais, bem como a necessidade de fortalecer as capacidades institucionais e judiciais, promovendo uma abordagem abrangente que combine sanções penais, prevenção, reparação às vítimas e educação digital.

Palavras-chave: Conteúdo íntimo não consensual, Deepfakes, Inteligência artificial, Regulamentação penal, Violência digital.

==== O ====

INTRODUCCIÓN

Dentro de un contexto de transformación digital, los cibercrímenes son ahora uno de los mayores riesgos para la seguridad personal, corporativa e incluso del estado. En palabras de Fernández y Martínez (2020), los actos de delincuencia cibernética, también conocidos como crimen informático, se engloban dentro de un delito socialmente categorizado que comprende actos que infringen los derechos de otros utilizando herramientas tecnológicas modernas. Tales acciones no solo son desagradables para la mayoría, sino que también están dentro del alcance del Derecho Penal debido al daño considerable que pueden infligir a la sociedad y al creciente uso de la tecnología en las actividades diarias.

Los ciberdelitos han evolucionado significativamente con el avance de la inteligencia artificial (IA), la cual ha transformado diversos sectores de la sociedad, incluido el entorno digital. El uso indebido de esta tecnología ha dado lugar a nuevas manifestaciones delictivas, como la creación y difusión de contenido manipulado mediante deepfakes. El término deepfake surgió en 2017 en foros digitales relacionados con la industria del entretenimiento, especialmente en Hollywood, y proviene de la combinación de las palabras deep (profundo) y fake (falso). Este concepto hace referencia a contenidos audiovisuales alterados mediante inteligencia artificial, en particular mediante algoritmos de aprendizaje profundo (deep learning), que permiten generar imágenes o videos extremadamente realistas, pero completamente falsos (Sinaluisa et al., 2024).

Aunque muchos videos producidos con tecnología deepfake capturan a individuos realizando actos que no parecen infringir su privacidad, el verdadero problema surge cuando estas herramientas se emplean de maneras dañinas. Particularmente impactante es la mejora del contenido pornográfico que circula en internet donde los rostros de personas reales se colocan sobre cuerpos ajenos en escenas explícitas sin su consentimiento. Esto ha causado un daño severo, especialmente a las mujeres, que constituyen aproximadamente el 96 por ciento de las víctimas de tales prácticas (De Moraes, 2020).

España ha avanzado en la regulación de estos crímenes con la Ley de Regulación de la Simulación de Imágenes y Voces de Personas Generadas por IA, que castiga el uso no autorizado de la imagen y la edición de video con inteligencia artificial. Además, la Unión Europea ha sido proactiva en la adopción del Reglamento Europeo de Servicios Digitales, que incorpora medidas de control y sanción para el uso indebido de deepfakes. En países como España, se ha establecido un marco de protección para las víctimas de deepfakes, otorgándoles acceso a canales de exposición prioritarios donde se prohíbe la difusión de materiales ilícitos.

Los deepfakes creados sin el consentimiento de la persona afectada vulneran gravemente derechos fundamentales como el honor, la intimidad y la reputación, al tiempo que refuerzan patrones de violencia de género digital. Si bien el Código Orgánico Integral Penal (COIP) (Asamblea Nacional del Ecuador, 2014) contempla figuras como la violación a la intimidad en su art. 178 y la suplantación de identidad en el art. 212, las cuales sancionan el acceso, difusión o publicación no autorizada de datos personales y la suplantación con fines de perjuicio, respectivamente, estas disposiciones no abarcan de manera específica ni suficiente la complejidad y particularidades de los deepfakes. La ausencia de una tipificación expresa para esta conducta genera un vacío normativo que limita la capacidad del sistema penal para sancionar eficazmente a quienes elaboran, difunden o comercializan este tipo de contenido ilícito, lo cual deja desprotegidas a las víctimas y obstaculiza una respuesta penal acorde con la gravedad del daño causado.

Aunque la Constitución ecuatoriana garantiza la protección de bienes jurídicos como la dignidad, la privacidad y la imagen, la ausencia de una figura penal concreta que abarque los deepfakes o deepnudes impide su sanción diferenciada dentro del ordenamiento jurídico. Esto provoca que las víctimas enfrenten serias dificultades para presentar denuncias efectivas, mientras que los infractores logran evadir responsabilidades penales, amparándose en la falta de tipificación expresa. Además, el principio de legalidad penal, nulla poena sine lege, establece que no puede imponerse pena sin una ley previa que defina la conducta punible, lo que perpetúa la impunidad en estos casos de violencia digital (Gamir Ríos y Tarullo, 2022). La falta de regulación en Ecuador no solo impide la protección efectiva de las víctimas, sino que también favorece la proliferación de ciberdelitos vinculados con la violencia digital, el ciberacoso y la explotación sexual, especialmente contra mujeres y menores de edad, quienes son las principales víctimas de este tipo de contenido ilícito.

Esta investigación resulta especialmente relevante porque contribuye al debate sobre la modernización del derecho penal ecuatoriano frente a los desafíos que plantean los

cibercrímenes y el uso de inteligencia artificial. Su propósito es evaluar no solo el impacto de estos delitos en las víctimas, sino también cómo afectan la confianza ciudadana en el sistema de justicia. Asimismo, busca identificar modelos regulatorios eficaces que puedan servir como referentes para futuras reformas legales en Ecuador.

La investigación también tiene como finalidad sensibilizar y capacitar a operadores judiciales y legisladores sobre la urgencia de establecer mecanismos de protección específicos para las víctimas de cibercrímenes, garantizando una respuesta jurídica adecuada a las complejidades del entorno digital. El objetivo central del estudio es analizar la necesidad de incorporar un tipo penal específico en el COIP para sancionar la creación y difusión de deepfakes sin consentimiento, determinando sus elementos estructurales, los sujetos activo y pasivo del delito, y las sanciones correspondientes, con base en la legislación española y las iniciativas normativas de la Unión Europea.

Metodología

La presente investigación se desarrollará bajo un enfoque cualitativo, dado que se centra en el análisis jurídico, doctrinario y normativo del fenómeno de los deepfakes y su tratamiento legal en el contexto ecuatoriano. Para ello, se emplearán los métodos de revisión bibliográfica, que permitirán recopilar y examinar literatura relevante en torno a los ciberdelitos, la inteligencia artificial y los derechos fundamentales afectados; el método analítico, con el fin de descomponer y examinar los elementos normativos y doctrinales del problema jurídico planteado; y el método de derecho comparado, a través del cual se estudiarán experiencias legislativas extranjeras, especialmente el caso de España y la Unión Europea, como referentes para una eventual reforma penal en Ecuador. El enfoque lógico será de tipo deductivo, ya que parte de principios generales del derecho penal, el marco constitucional y legal vigente, para llegar a conclusiones específicas respecto a la necesidad de una regulación penal especial sobre la creación y difusión de deepfakes sin consentimiento.

DESARROLLO

Delitos Digitales análisis desde la teoría del delito

Los delitos digitales son un fenómeno relativamente reciente, pero de rápida expansión, que surge como resultado del avance acelerado de las tecnologías de la información y la comunicación. A medida que las sociedades se volvieron más dependientes de la tecnología para llevar a cabo actividades cotidianas, laborales y sociales, también comenzaron a surgir formas de criminalidad adaptadas a este nuevo entorno virtual. Para Wall (2007), los delitos digitales engloban aquellas conductas ilícitas que utilizan las tecnologías informáticas como instrumento o finalidad, caracterizándose por su complejidad técnica, su alcance transnacional y su potencial para afectar a múltiples víctimas simultáneamente.

El origen de los delitos digitales puede rastrearse a los primeros incidentes de intrusión no autorizada a sistemas informáticos en las décadas de 1970 y 1980, cuando se manipularon bases de datos o sistemas financieros incipientes. Sin embargo, su expansión global se consolidó con el auge del internet comercial en los años 90, cuando el correo electrónico, las redes sociales y la navegación en línea comenzaron a masificarse. Como explica Brenner (2010), la evolución tecnológica ha impulsado la transformación constante de los delitos digitales, que se adaptan a las nuevas herramientas y a la creciente conectividad global, aprovechando el anonimato y las dificultades para su rastreo en el ciberespacio.

El aspecto más particular de estos delitos es que se ejecutan en un espacio intangible, lo que permite a los agresores operar desde cualquier lugar del mundo y ocultar con facilidad su identidad. Según McGuire (2012), la amenaza real de la ciberdelincuencia no solo radica en su sofisticación técnica, sino en su capacidad para difundir desinformación, manipular la

opinión pública y erosionar la confianza en los sistemas digitales. Esta característica hace que las víctimas a menudo no perciban la vulneración hasta sufrir consecuencias económicas, reputacionales o psicológicas significativas. Wall (2007) coincide en que tanto delincuentes individuales como grupos organizados utilizan estas plataformas para perpetrar fraudes, chantajes, suplantaciones y manipulaciones mediáticas, empleando herramientas que anteriormente estaban reservadas a expertos técnicos.

Con el paso del tiempo, los delitos digitales se han diversificado considerablemente. Existen ciberdelitos orientados al fraude, como el phishing o el robo de credenciales bancarias; otros dirigidos a la identidad, como la suplantación en redes sociales; y formas de violencia digital, como el acoso en línea, la sextorsión y la difusión no consentida de imágenes íntimas. Un fenómeno reciente es el empleo de inteligencia artificial para crear contenidos falsos, denominados deepfakes, usados para difamación, manipulación política o violencia simbólica de género (Chesney y Citron, 2019). Estas modalidades muestran que la tecnología no solo es un instrumento, sino que redefine las dinámicas delictivas y la manera en que las personas interactúan con el riesgo.

Uno de los retos más complejos de los delitos digitales es su rápida transformación. Como indican Wall y Williams (2013), cada innovación tecnológica genera nuevas vulnerabilidades que pueden ser explotadas por actores maliciosos para cometer delitos de formas novedosas y difíciles de detectar. El uso de algoritmos avanzados, criptomonedas, redes descentralizadas y plataformas en la nube ha permitido a los ciberdelincuentes operar con esquemas cada vez más complejos. Asimismo, la dependencia creciente de dispositivos móviles e hiperconectividad facilita que los ataques tengan consecuencias masivas en segundos.

Los efectos de estos delitos son amplios y profundos. No solo implican pérdidas económicas o patrimoniales, sino que también causan daños emocionales, sociales y simbólicos. McGuire (2012) sostiene que la ciberdelincuencia ataca uno de los pilares fundamentales de la vida moderna: la confianza. Las víctimas pueden experimentar miedo, ansiedad, humillación o aislamiento, especialmente en casos de violencia digital o manipulación de su imagen. Además, el contenido digital, una vez difundido, puede replicarse sin control, incrementando el daño y la sensación de indefensión. Según Chesney y Citron (2019), uno de los aspectos más angustiosos es la naturaleza persistente de estos contenidos, que, aunque sean retirados de ciertas plataformas, pueden seguir circulando en otras o almacenados en dispositivos privados.

El anonimato constituye otra característica clave de estos delitos. Para Brenner (2010), el entorno digital posibilita que los agresores actúen tras un velo de anonimato, dificultando su identificación y aumentando su capacidad de intimidación o manipulación. Esta ventaja se amplifica por la falta de habilidades digitales en muchas víctimas, generando un claro desequilibrio operativo. Además, el actuar en múltiples jurisdicciones confiere a los delitos digitales una dimensión global, complicando las labores de prevención y persecución.

Los delitos digitales deben entenderse como una extensión inevitable de los cambios culturales y tecnológicos de la sociedad actual. El ciberespacio ha transformado conceptos tradicionales de propiedad, privacidad, identidad y reputación. En este sentido, Wall (2007) argumenta que los espacios digitales han dejado de ser entornos paralelos para convertirse en escenarios reales de la vida social, económica y emocional. Por ello, los delitos cometidos en estos ámbitos no deben subestimarse, pues sus impactos son reales, duraderos y frecuentemente irreversibles. Los delitos digitales deben entenderse no como una categoría aislada, sino como una extensión inevitable de los cambios culturales y tecnológicos de la sociedad contemporánea. El ciberespacio ha transformado las nociones tradicionales de propiedad, privacidad, presencia y reputación. Anderson (2018) sostiene que los entornos digitales han dejado de ser espacios paralelos o virtuales para convertirse en escenarios reales de la vida social, económica y emocional. Por ello, los delitos que allí se cometen no

deben subestimarse, ya que sus impactos son reales, duraderos y muchas veces irreversibles.

Desde la perspectiva de la teoría del delito, la conducta típica en los delitos digitales consiste en la realización de actos que involucran un elemento informático o telemático, como ocurre con el acceso indebido a sistemas o la manipulación de datos (Davara Rodríguez, 2002). Esta tipicidad se ve afectada por la carencia, en algunos ordenamientos, de tipos específicos para estos comportamientos, lo que obliga a recurrir a interpretaciones extensivas o analógicas que, como advierte Acurio Del Pino (2016), pueden entrar en tensión con el principio de legalidad. En efecto, la jurisprudencia ha debido equilibrar la necesidad de tutelar bienes jurídicos emergentes con el respeto a la seguridad jurídica y a los principios garantistas del derecho penal.

La antijuridicidad en estos delitos se configura cuando se vulneran bienes jurídicos como la intimidad, el patrimonio o la seguridad nacional, pero también la confianza social en el uso de las tecnologías, un bien jurídico colectivo que no siempre ha sido reconocido expresamente (Acurio Del Pino, 2016). De hecho, autores como Pérez Luño (1996) han sostenido que la información y la confianza en los sistemas informáticos deben considerarse bienes jurídicos autónomos en la sociedad de la información, debido a su importancia económica y social. Esto obliga a repensar la función de la antijuridicidad, entendida no solo como la afectación de intereses individuales sino también de valores sociales y económicos de gran trascendencia.

La imputabilidad en los delitos digitales no siempre recae en expertos informáticos. Si bien el perfil del sujeto activo suele vincularse a habilidades técnicas, Acurio Del Pino (2016) advierte que muchos de estos delitos son cometidos por personas con acceso privilegiado a los sistemas (insiders), aunque también pueden ser perpetrados por individuos con conocimientos básicos gracias a la creciente disponibilidad de herramientas tecnológicas. Asimismo, opina Tiedemann (1996), esta democratización de la tecnología plantea retos para la política criminal, ya que facilita la comisión de delitos por personas ajenas al ámbito profesional informática. Así, la culpabilidad debe analizarse considerando no solo el conocimiento técnico, sino también la voluntad consciente de vulnerar los sistemas o datos protegidos.

En cuanto al bien jurídico protegido, los delitos digitales son esencialmente pluriofensivos, ya que pueden afectar simultáneamente la intimidad, el patrimonio y la seguridad de los sistemas. Gutiérrez Francés (2002) sostiene que estas conductas provocan una doble afección: a intereses económicos y a intereses colectivos vinculados al correcto funcionamiento de los sistemas informáticos. Este enfoque resalta la necesidad de que la teoría del delito reconozca la naturaleza compleja de estas infracciones y la interrelación de bienes jurídicos afectados.

La tradicional estructura de acción típica, antijuridicidad y culpabilidad sigue siendo válida, pero debe complementarse con categorías más dinámicas que permitan entender fenómenos como la neutralización de la conducta delictiva o la dificultad de imputar resultados en entornos digitales.

Cuando se hace referencia a la necesidad de incorporar categorías más dinámicas dentro de la teoría del delito, se alude a la urgencia de actualizar los marcos tradicionales para enfrentar los desafíos específicos que plantea el entorno digital. Estas categorías pueden incluir, por ejemplo, nuevas formas de analizar la imputación objetiva cuando la acción se produce mediante algoritmos o sistemas automatizados, o enfoques que consideren el dolo en contextos donde la intención puede estar mediada por conductas colectivas y anónimas en redes (Johnson y Diakopoulos, 2021). La "neutralización" de la conducta delictiva entendida como una forma de autojustificación del autor cobra relevancia cuando ciertos agentes digitales apelan a discursos como la "ética hacker", según la cual el acceso no

autorizado a sistemas informáticos puede considerarse legítimo si persigue fines como la transparencia, la justicia social o el beneficio público. Estas nuevas realidades exigen repensar la manera en que se configura la responsabilidad penal, especialmente en escenarios donde la causalidad es difícil de establecer debido al carácter global, descentralizado y técnico del ciberespacio.

Deepfakes y contenido íntimo no consentido

Los deepfakes son contenidos audiovisuales generados mediante técnicas de inteligencia artificial, particularmente por redes generativas antagónicas o GANs, que permiten la creación de imágenes, videos o audios hiperrealistas y falsificados. Su nombre proviene de la combinación de deep learning que significa aprendizaje profundo y fake que es falsificación. Según García (2021), "los deepfakes son vídeos hiperrealistas manipulados digitalmente para representar a personas que dicen y hacen cosas que en realidad nunca dijeron ni sucedieron" (p. 107). Esta tecnología, aunque inicialmente concebida con fines lúdicos o artísticos, ha dado lugar a una serie de preocupaciones éticas y legales debido a sus múltiples aplicaciones potencialmente nocivas.

El primer escenario ampliamente conocido de un deepfake se produjo en 2017, cuando un usuario de la plataforma Reddit, bajo el seudónimo "Deepfakes", difundió videos pornográficos en los que superponía rostros de celebridades como Gal Gadot, Maisie Williams o Taylor Swift en cuerpos de actrices del cine para adultos, utilizando un algoritmo de machine learning en su propia computadora (Del Campillo, 2021; García-Ull, 2021). Esta práctica se viralizó rápidamente, demostrando el bajo umbral técnico necesario para producir este tipo de contenido y generando un precedente alarmante para la privacidad e integridad digital de las personas. Como señalan Cerdán y Padilla (2019), estos contenidos son especialmente problemáticos por su grado de realismo y por la dificultad para discernir su carácter falso.

A partir de allí, surgieron aplicaciones como FaceApp, que permiten a cualquier persona modificar rostros, añadir expresiones o cambiar edades y géneros. Esta facilidad técnica democratizó la producción de deepfakes y multiplicó su uso, incluso en escenarios de manipulación política. Un ejemplo de ello fue el engaño a diputados europeos en 2021 mediante una videollamada con un deepfake de Leonid Volkov, opositor al gobierno ruso (Del Campillo, 2021). Otro caso emblemático ocurrió cuando el presidente ucraniano Volodímir Zelenski tuvo que desmentir un video en el que su imagen adulterada pedía a sus tropas rendirse ante Rusia.

En cuanto a su funcionamiento técnico, García-Ull (2021) describe que estas representaciones sintéticas son el producto de redes neuronales artificiales que se enfrentan en un sistema de entrenamiento recíproco, donde una red generadora crea contenido falso mientras otra intenta detectarlo, mejorando mutuamente hasta lograr un producto visual o auditivo que resulta extremadamente verosímil (p. 107-108). Esta sofisticación técnica representa una amenaza para la confianza pública en la información visual y sonora, al punto de que incluso los sentidos humanos se ven superados, dificultando la distinción entre lo real y lo ficticio (Cerdán et al., 2020).

La creación y difusión de deepfakes sexuales sin consentimiento constituye una nueva forma de violencia de género digital, en la cual se vulnera la imagen, la privacidad y la dignidad de las víctimas. Henry et al. (2021) afirman que este tipo de agresión puede equipararse a formas tradicionales de abuso sexual, ya que se invade simbólicamente el cuerpo y la identidad de la víctima, produciendo consecuencias psicológicas devastadoras, aunque no haya contacto físico. En este sentido, la utilización de deepfakes para propósitos sexuales sin consentimiento trasciende el ámbito de lo tecnológico y se convierte en una herramienta de dominación, cosificación y humillación.

El informe de Sensity AI reveló que hasta el año 2020, el 96% de los deepfakes detectados en Internet eran de naturaleza pornográfica, afectando principalmente a mujeres (Goriup et al., 2019). Esta estadística demuestra no solo una evidente desigualdad de género en el uso nocivo de esta tecnología, sino también una alarmante tendencia a la cosificación digital del cuerpo femenino, donde las mujeres son objeto de fantasías masculinas producidas y difundidas sin su consentimiento. El impacto en la salud mental, la reputación y la vida personal de las víctimas es innegable, y muchas veces irreversible, considerando que una vez compartido, el contenido puede quedar alojado en múltiples servidores o dispositivos, fuera del control individual.

En el plano jurídico, las normas tradicionales sobre privacidad, honra y derechos a la imagen han demostrado ser insuficientes frente a la sofisticación y velocidad con que se producen y difunden los deepfakes. Como advierten Chesney y Citron (2019), los marcos legales actuales son inadecuados para responder eficazmente a esta amenaza emergente, por lo que proponen reformas integrales que incluyan la tipificación específica de los deepfakes nocivos, la imposición de obligaciones a las plataformas digitales, y el fortalecimiento de los derechos digitales y de la protección a la identidad.

Por otra parte, la UNESCO (2021) ha señalado la necesidad urgente de establecer estándares internacionales que regulen el uso ético de estas tecnologías, promoviendo una inteligencia artificial centrada en los derechos humanos. Esta perspectiva encuentra sustento en la doctrina jurídica contemporánea, que subraya la importancia de reconocer y proteger nuevos derechos digitales, como la identidad digital, la autodeterminación informativa y el derecho al olvido.

En cuanto a los actores involucrados, Floridi (2018) y García-Ull (2021) identifican cuatro tipos fundamentales: i) comunidades de aficionados, que utilizan la tecnología con fines de entretenimiento o experimentación técnica; ii) actores políticos, que emplean los deepfakes como herramientas de manipulación informativa en campañas electorales o conflictos geopolíticos; iii) delincuentes y estafadores, que recurren a estos recursos para chantaje, fraude o extorsión; y iv) actores legítimos, como artistas, cineastas o educadores, que exploran usos éticos para recreaciones históricas, efectos especiales o protección de identidad. Bañuelos y Gómez (2020) propone una clasificación de los ámbitos más afectados por los deepfakes, señalando el entretenimiento, la política, el campo experimental y, de forma destacada, el ámbito pornográfico como los principales escenarios de su proliferación.

Pese a los posibles usos positivos, como la preservación del anonimato de víctimas en procesos judiciales o la recreación histórica con fines educativos, la balanza actual se inclina hacia un uso predominantemente negativo. Esta tendencia se ve agravada por la falta de controles efectivos en las plataformas, la rápida viralización del contenido y la dificultad para su eliminación (Del Campillo, 2021). Además, la pérdida de confianza en la autenticidad de la información visual y auditiva socava la estructura misma de la democracia, al afectar la percepción ciudadana y la toma de decisiones informadas (Gómez y Escobar, 2021).

Las visiones más pesimistas coinciden en que los deepfakes serán utilizados con creciente frecuencia para la pornografía de venganza, la manipulación política, la propaganda extremista, el chantaje o incluso como prueba falsa en juicios (García-Ull, 2021). Frente a esta realidad, se impone la necesidad de un enfoque interdisciplinario que articule regulación jurídica, alfabetización digital, ética tecnológica y responsabilidad de las plataformas, para evitar que el deepfake se convierta en un arma de destrucción de la verdad, la dignidad y la justicia.

En Ecuador, esta problemática representa una amenaza directa al derecho a la intimidad, reconocido como un derecho fundamental por la Constitución de la República. La manipulación de imágenes o videos mediante inteligencia artificial para superponer el rostro

de una persona sobre un cuerpo ajeno en escenas sexuales explícitas, sin su consentimiento, vulnera de forma directa la integridad personal y el bienestar psicológico de las víctimas, afectando su honra, imagen pública y derechos fundamentales como el de protección de datos personales y el respeto a su vida privada.

El ordenamiento jurídico ecuatoriano aún no contempla una tipificación penal específica que sancione la creación y difusión de deepfakes, a pesar de que en la Constitución de la República del Ecuador 2008 (Asamblea Nacional Constituyente, 2008) constan como derechos; "El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona" (art. 66.18) y "El derecho a la intimidad personal y familiar" (art. 66.20). Esta omisión no solo dificulta la prevención y sanción de conductas lesivas, sino que también limita el acceso efectivo a la justicia para las personas afectadas. Resulta indispensable avanzar hacia una regulación que no solo reconozca los derechos vulnerados, sino que contemple mecanismos específicos para su protección en el entorno digital.

Aunque existen normas que podrían aplicarse de forma supletoria en estos casos, como el artículo 178 del COIP, que indica:

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.

Esta norma está diseñada para casos de acceso o difusión no autorizada de información real y preexistente, mientras que los deepfakes implican la manipulación o generación de contenido falso que simula ser auténtico. Es decir, no se trata de una simple divulgación de datos personales, sino de la creación deliberada de material engañoso que puede dañar la reputación, la dignidad y otros derechos fundamentales. Por tanto, aplicar esta norma de forma supletoria no permite abordar con precisión la complejidad ni la gravedad del fenómeno, lo que deja un margen de impunidad y una brecha en la tutela efectiva de derechos.

Por ello, De Moraes (2020) revela que existe un vacío normativo en Ecuador frente al uso de deepfakes pornográficos, lo cual se traduce en dificultades probatorias al momento de judicializar estos casos. La inexistencia de peritos especializados en inteligencia artificial y en técnicas de análisis forense digital complica la identificación del origen de los contenidos falsificados y, por tanto, la atribución de responsabilidad penal. Además, los métodos tradicionales de investigación penal no están preparados para rastrear direcciones IP, analizar cuentas espejo o descomponer estructuras algorítmicas complejas utilizadas en la creación de estos videos manipulados. En consecuencia, el documento concluye que es necesario reformar el COIP para incorporar un tipo penal autónomo que regule el uso malicioso de estas tecnologías y que se fortalezcan las capacidades institucionales del sistema judicial en materia de cibercriminalidad (Sinaluisa et al., 2024).

Un dato preocupante que se recoge en la investigación es que más del 86% de los fiscales, jueces y defensores especializados en víctimas consultados consideran que los deepfakes representan una amenaza significativa al derecho a la intimidad, y más del 93% reconoce que su difusión puede causar daños psicológicos y emocionales graves en las personas afectadas. Sin embargo, más del 80% cree que la legislación ecuatoriana actual no aborda adecuadamente esta problemática, y el 73% opina que el sistema judicial no está preparado para enfrentar este tipo de delitos tecnológicos (Gamir Ríos y Tarullo, 2022).

España ha adoptado un enfoque más proactivo frente al uso de deepfakes pornográficos. La Ley 13/2022 General de Comunicación Audiovisual prohíbe la difusión de contenidos manipulados sin consentimiento, considerándolo una infracción grave cuando se atenta contra la integridad o la dignidad de las personas afectadas. Además, el Código Penal español ha incorporado reformas que reconocen los deepfakes como "ultrafalsificaciones", lo que permite su persecución penal como delitos autónomos, con penas que pueden alcanzar hasta nueve años de prisión (Corte General, 2022; Marcus, 2024).

España también cuenta con un marco jurídico sólido en cuanto a la protección de datos personales, gracias a la Ley Orgánica 3/2018, que establece principios como el consentimiento informado, el derecho al olvido y la protección de la imagen personal. Esta normativa ha permitido sancionar la creación y difusión de videos sexualmente explícitos generados mediante inteligencia artificial cuando estos afectan la privacidad de las personas. Adicionalmente, España participa activamente en iniciativas internacionales como el Convenio de Budapest sobre Ciberdelincuencia, lo que facilita la cooperación judicial transnacional en la persecución de estos delitos (Sinaluisa et al., 2024).

La respuesta española al fenómeno de los deepfakes también incluye un componente educativo y preventivo. Se han desarrollado campañas de concientización digital sobre los riesgos de compartir imágenes personales en línea y se han impulsado programas de formación para fiscales, jueces y cuerpos de seguridad sobre detección de manipulaciones digitales. A diferencia de Ecuador, donde aún se carece de protocolos técnicos específicos, en España se emplean pericias audiovisuales avanzadas para detectar inconsistencias en los parpadeos, expresiones faciales y movimientos de labios, que permiten determinar si un video ha sido alterado por inteligencia artificial (Ehrenkranz, 2018; Anderson, 2018).

Desde una perspectiva comparativa, resulta evidente que España ha logrado integrar el fenómeno de los deepfakes dentro de su política penal y de protección de derechos digitales, mientras que Ecuador todavía se encuentra en una etapa exploratoria, con propuestas de reforma y diagnósticos institucionales que no han sido formalizados en una legislación específica.

Propuesta de Regulacion Penal en Ecuador

La creciente problemática de los deepfakes con contenido íntimo no consentido en Ecuador exige la creación de una regulación penal específica que contemple las particularidades técnicas y sociales de este fenómeno. La ausencia de un tipo penal autónomo en el COIP genera vacíos legales que dificultan la protección efectiva de los derechos fundamentales de las víctimas, principalmente la intimidad, la dignidad y la protección de datos personales. En este contexto, resulta indispensable que la normativa penal contemple de manera clara y precisa la tipificación del delito relacionado con la creación, distribución y difusión de contenido audiovisual manipulado mediante inteligencia artificial sin el consentimiento de la persona afectada.

El tipo penal propuesto debería describir como conducta típica la generación, producción, almacenamiento, publicación o difusión de imágenes, videos o audios falsificados que representen a una persona en situaciones sexuales explícitas o íntimas, sin su autorización expresa. Esta conducta debe contemplar no solo la reproducción del contenido sino también la facilitación y promoción en plataformas digitales. La penalización debe ser proporcional al daño causado, considerando agravantes como la reiteración, la participación de menores, la difusión masiva o el uso con fines de extorsión o chantaje. En consonancia con la doctrina penal contemporánea, la tipificación debe garantizar que la conducta sea evaluada en su contexto digital, contemplando la complejidad técnica del deepfake y la potencialidad de daño simbólico y psicológico que genera (Chalcraft, 2021).

Respecto a los sujetos activos, se debe incluir tanto a quienes directamente generan el contenido falsificado mediante técnicas de inteligencia artificial, como a quienes lo difunden,

distribuyen o comercializan sin consentimiento, abarcando así a productores, intermediarios y plataformas digitales cuando actúen con dolo o negligencia grave. En cuanto a los sujetos pasivos, claramente se trata de las personas cuya imagen, voz o identidad digital es utilizada sin autorización para crear deepfakes sexuales, siendo estas víctimas de una forma específica de violencia digital que afecta su esfera íntima y personal (Henry et al., 2021). Además, la ley debe proteger a las personas jurídicas cuando se utilicen sus imágenes o datos de forma ilícita, en caso de vulneración de derechos corporativos o de marca.

La necesidad de una norma específica radica en la insuficiencia de las disposiciones actuales para abordar las particularidades del delito. Como advierten Delva y González (2022), las normas generales sobre privacidad o violación a la intimidad no alcanzan a cubrir la complejidad técnica ni la rapidez con que se producen y propagan los deepfakes. La inteligencia artificial introduce nuevas dinámicas de creación y difusión que requieren una respuesta legal adaptada, que incluya no solo sanciones penales sino también medidas de prevención, reparación y protección de las víctimas. Una regulación específica también es vital para fortalecer las capacidades investigativas y judiciales, incentivando la capacitación en análisis forense digital y la cooperación interinstitucional para enfrentar eficazmente estos delitos.

La tipificación autónoma debe contribuir a visibilizar esta modalidad de violencia de género digital, reconociéndola como un atentado grave contra la dignidad y la autonomía personal. El impacto psicológico y social que sufren las víctimas exige una respuesta integral que combine la sanción penal con mecanismos de reparación, atención psicológica y protección de derechos digitales. Esta visión multidimensional de la regulación penal se sustenta en propuestas internacionales que buscan armonizar la protección de los derechos humanos con el desarrollo tecnológico.

La incorporación de un tipo penal específico en el COIP dedicado a los deepfakes sexuales no consentidos es una medida imprescindible para garantizar la justicia en la era digital. Este tipo penal debe ser preciso, contemplar todos los actos relacionados con la producción y difusión, establecer sujetos activos y pasivos claros, y prever sanciones proporcionales que reflejen la gravedad del daño. Solo a través de una norma especializada, que reconozca las particularidades técnicas y humanas de estos delitos, Ecuador podrá ofrecer una protección efectiva a las víctimas y enfrentar adecuadamente este desafío emergente en la cibercriminalidad contemporánea.

La regulación penal específica para los deepfakes con contenido íntimo no consentido en Ecuador es imprescindible para cerrar los vacíos legales que actualmente dificultan la protección efectiva de la intimidad, la dignidad y otros derechos fundamentales de las víctimas. Es necesario incorporar un tipo penal autónomo en el COIP que contemple no solo la producción y difusión de este tipo de material, sino también la responsabilidad penal de todos los actores involucrados en su creación, distribución y promoción. Basándose en el principio de proporcionalidad y considerando que el bien jurídico vulnerado es el derecho a la intimidad, se propone una sanción privativa de libertad de tres a cinco años, agravándose si el contenido generado causa daños psicológicos severos, afecta a menores de edad o tiene una amplia difusión. Además, la norma debe incluir mecanismos de reparación integral para las víctimas y fortalecer la capacidad judicial frente a esta nueva forma de violencia digital, en concordancia con los estándares internacionales de derechos humanos y justicia tecnológica.

DISCUSIÓN

El fenómeno de los deepfakes con contenido íntimo no consentido expone una clara brecha entre el avance tecnológico y la capacidad regulatoria del sistema jurídico ecuatoriano. La sofisticación de las técnicas de inteligencia artificial, como las redes generativas antagónicas (GANs), ha superado la respuesta normativa tradicional que Ecuador posee, evidenciando la

insuficiencia de las disposiciones actuales para proteger la intimidad y dignidad de las personas frente a este tipo de ciberdelitos. Este desfase legal genera espacios de impunidad y vulnerabilidad para las víctimas, dificultando la persecución penal y la reparación integral, y pone en evidencia la necesidad imperiosa de reformar el Código Orgánico Integral Penal para incluir un tipo penal específico que contemple las particularidades técnicas y sociales del deepfake sexual no consentido.

Más allá del daño material o económico, los deepfakes íntimos no autorizados constituyen una forma grave de violencia de género digital que atenta contra derechos fundamentales, tales como la autonomía personal, la privacidad y la dignidad. En el contexto ecuatoriano, donde las estructuras sociales aún reflejan profundas desigualdades de género, esta modalidad de violencia se convierte en un mecanismo de dominación simbólica que perpetúa la cosificación y la humillación pública de las víctimas, causando daños psicológicos que pueden ser duraderos y complejos de abordar. Esta dimensión simbólica y emocional exige que la regulación penal no solo sancione el acto ilícito, sino que también contemple medidas de reparación, atención integral a las víctimas y acciones de prevención.

La regulación penal específica que se propone debe entenderse como parte de un enfoque multidisciplinario y coordinado que involucre no solo la tipificación clara y punitiva del delito, sino también la capacitación técnica de operadores de justicia, la incorporación de peritos en inteligencia artificial y análisis forense digital, y el diseño de estrategias educativas para promover la alfabetización digital y la prevención en la sociedad. Sin estas acciones complementarias, la sola existencia de una norma penal resultaría insuficiente para garantizar la protección efectiva y la justicia para las víctimas.

La persecución penal de los deepfakes enfrenta múltiples desafíos probatorios derivados de la complejidad técnica y la velocidad con que se generan y viralizan estos contenidos. La falta de peritos especializados y protocolos actualizados limita la capacidad del sistema judicial ecuatoriano para identificar y atribuir responsabilidades, lo que se traduce en una baja tasa de judicialización y condenas efectivas. Por ello, la reforma legislativa debe ir acompañada de un fortalecimiento institucional que facilite el desarrollo de capacidades técnicas y la cooperación interinstitucional en la lucha contra la ciberdelincuencia.

En cuanto a la responsabilidad de las plataformas digitales, la regulación debe incluir disposiciones claras que exijan a los proveedores de servicios y redes sociales implementar mecanismos efectivos para la detección y remoción inmediata de deepfakes no consentidos. Esta medida es crucial para frenar la rápida propagación y el daño masivo que estos contenidos pueden generar, aunque se debe preservar un equilibrio que garantice el respeto a la libertad de expresión y la privacidad, evitando censuras arbitrarias. El papel activo de las plataformas es fundamental en un ecosistema digital donde la viralización puede multiplicar exponencialmente el impacto negativo sobre las víctimas.

La comparación con experiencias internacionales, como la regulación española o los lineamientos éticos de la UNESCO, revela que una política penal robusta puede ser un instrumento eficaz para proteger derechos y sancionar conductas ilícitas relacionadas con deepfakes. España, por ejemplo, ha incorporado reformas específicas que permiten perseguir penalmente la creación y difusión de deepfakes pornográficos, junto con un marco sólido de protección de datos y derechos digitales que contribuyen a un abordaje integral. Adaptar estas buenas prácticas al contexto ecuatoriano, considerando las particularidades sociales y jurídicas, puede ofrecer una hoja de ruta para avanzar hacia una regulación efectiva y justa.

Es imprescindible abordar las profundas implicaciones éticas y sociales que plantea el uso de la inteligencia artificial para generar contenido íntimo falso. Más allá de la esfera jurídica, este fenómeno impacta en la confianza social, la reputación de las personas y la percepción de la realidad, erosionando el valor de la información visual y sonora como fuente confiable.

La regulación penal, por tanto, debe ser acompañada por un debate público y una reflexión ética que promuevan la responsabilidad colectiva frente a los riesgos que plantea la tecnología, fomentando una cultura digital basada en el respeto, la protección y la dignidad humana.

LIMITACIONES DEL ESTUDIO

El presente estudio, si bien aborda una problemática crítica y actual en el ámbito legal, presenta ciertas limitaciones inherentes a su naturaleza y alcance. Una de las principales restricciones es la falta de datos estadísticos oficiales y específicos sobre la incidencia de delitos digitales de contenido íntimo generado por inteligencia artificial en Ecuador. Al ser un fenómeno relativamente reciente y con un vacío normativo, los casos no suelen ser tipificados de forma clara, lo que dificulta la cuantificación precisa de su prevalencia. Esto nos obligó a basar gran parte de nuestro análisis en estudios internacionales y en encuestas a un grupo limitado de operadores de justicia, lo que podría no reflejar la totalidad del panorama nacional.

ESTUDIOS FUTUROS

A partir de las conclusiones y limitaciones de esta investigación, se abren varias líneas de estudio que podrían fortalecer la comprensión y el abordaje de los delitos digitales de contenido íntimo. Sería fundamental realizar una investigación cuantitativa a gran escala que, a través de encuestas anónimas a la población, permita dimensionar el alcance real de la victimización por *deepfakes* en Ecuador. Asimismo, se sugiere un estudio de derecho comparado más profundo, analizando no solo la legislación de España, sino también la de otros países que han implementado regulaciones exitosas para combatir este tipo de ciberdelitos. Finalmente, se propone investigar los mecanismos de cooperación internacional entre las autoridades judiciales y las plataformas tecnológicas, a fin de establecer protocolos efectivos para la remoción de contenido y la persecución de los responsables en un entorno digital global.

RECONOCIMIENTO

Agradecemos profundamente el apoyo y la dedicación de quienes contribuyeron a la realización de este artículo. Expresamos nuestra especial gratitud a los docentes de la Carrera de Derecho de la Universidad Tecnológica Indoamérica, cuyo compromiso con la investigación fue fundamental. De igual modo, reconocemos el valioso aporte de los colegas especialistas y profesionales que, con sus conocimientos y experiencia, enriquecieron el análisis y las conclusiones de este trabajo.

APORTE DE LOS COAUTORES

- **Lilia Margarita Taco Sánchez:** Encargada del diseño metodológico del estudio, incluyendo la elaboración del esquema de investigación. Realizó la exhaustiva búsqueda y síntesis de la información, sirviendo de base para la redacción del borrador inicial del manuscrito.
- **Francisco David Villacís Mogrovejo:** En su rol de asesor, orientó y supervisó el proceso completo de la investigación. Su valiosa retroalimentación y sugerencias fueron clave para la revisión y perfeccionamiento del manuscrito final.

CONCLUSIONES

Los delitos digitales representan una manifestación novedosa y compleja del fenómeno delictivo, que surge y se expande paralelamente al avance tecnológico y la creciente dependencia social de las tecnologías de la información. Desde la teoría del delito, estos

crímenes desafían las categorías tradicionales al involucrar bienes jurídicos emergentes como la confianza en los sistemas digitales y afectar simultáneamente la intimidad, el patrimonio y la seguridad colectiva. La diversidad de perfiles de los sujetos activos, gracias a la democratización tecnológica, exige un análisis dinámico de la imputabilidad y culpabilidad, mientras que la rápida evolución de las modalidades delictivas impone la urgente necesidad de actualizar los marcos legales con tipos penales específicos, sin menoscabar principios fundamentales como el de legalidad. En suma, para enfrentar eficazmente esta realidad, es imprescindible que la política criminal evolucione para proteger los derechos fundamentales y garantizar la seguridad y confianza en el entorno digital.

Los deepfakes y la difusión de contenido íntimo no consentido representan una grave amenaza para la privacidad, la dignidad y la integridad psicológica de las víctimas, constituyendo una nueva forma de violencia de género digital que exige atención urgente desde el ámbito jurídico y social. Aunque esta tecnología tiene potenciales usos legítimos, su proliferación ha sido mayoritariamente perjudicial, facilitando la creación de imágenes y videos falsificados con un alto grado de realismo que dificulta su detección y combate. En Ecuador, la ausencia de una tipificación penal específica para estos delitos, sumada a limitaciones técnicas y normativas, dificulta la persecución efectiva y protección de los derechos afectados. En contraste, países como España han avanzado con regulaciones claras y mecanismos de detección especializados, combinando medidas legales, educativas y preventivas que podrían servir de referencia para fortalecer la respuesta ecuatoriana. Por tanto, es imprescindible impulsar reformas legales integrales que contemplen la naturaleza y alcance de los deepfakes sexuales no consentidos, al mismo tiempo que se promueven políticas públicas interdisciplinarias para proteger a las víctimas y preservar la confianza en la información digital.

REFERENCIAS

Anderson, K. E. (2018). Getting acquainted with social networks and apps: Combating fake news on social media. Library Hi Tech News, 35(3), 1–6. https://doi.org/10.1108/lhtn-02-2018-0010

Asamblea Nacional Constituyente (2008). Constitucion de la República del Ecuador. Url: https://www.lexis.com.ec › biblioteca › constitucion-republica-ecuador

Asamblea Nacional del Ecuador (2014). Código Orgánico Integral Penal (COIP) - Asamblea Nacional. Url: https://www.asambleanacional.gob.ec › es › system › files › document.pdf

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.

Bañuelos, J., & Gómez, A. (2020). Visualidad totalizante. *Revista Mexicana de Comunicación*, (145), 16.

Cerdán Martínez, V. M., García Guardia, M. L., & Padilla Castillo, G. (2020). Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales. Cuadernos de Información y Comunicación 25, 165-181

Chalcraft, D. (2021). Artificial Intelligence and Criminal Liability: The Case of Deepfakes. Journal of Digital Law, 12(3), 45-67.

Chesney, R., & Citron, D. K. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs, 98(1), 147-155.

Corte General. (2022). Ley General de Comunicación Audiovisual. España.

Davara Rodríguez, M. A. (2002). La Ley de Servicios de la Información y el Comercio Electrónico. *Otrosí, Revista informativa del Ilustre Colegio de Abogados de Madrid*, (41), 38-45.

De Moraes, C. P. (2020). "Deepfake" como ferramenta de manipulação e disseminação de "fakenews" em formato de vídeo nas redes sociais. *Biblios: Revista electrónica de bibliotecología, archivología y museología*, (79), 5.

del Campillo, S. G. (2021). Blockchain: una revolución de vieja data. *Revista Blockchain e Inteligencia Artificial*, (2).

Del Pino, S. A. (2016). Delitos informáticos: generalidades. Universidad de Sna Marcos. Costa Rica. URI: localhost/xmlui/handle/11506/2374

Delva, J. y González, I. (2022). Venta sexual digital: las redes sociales y su regulación internacional. Jurídicas CUC, 18(1), 241–278. DOI: http://dx.doi.org/10.17981/juridcuc.18.1.2022.11

Ehrenkranz, M. (2018, 16 de junio). Hay un truco infalible para detectar si un vídeo ha sido manipulado por una IA Deep Fake: fíjate en los ojos. Gizmodo en Español. https://es.gizmodo.com/hay-un-truco-infalible-para-detectar-si-un-video-ha-sid-1826888894

Fernández Bermejo, D. & Martínez Atienza, G. (2020). Ciberdelitos: (ed.). Ediciones Experiencia. https://elibro.net/es/lc/uti/titulos/167811

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180081.

Gamir Ríos, J., & Tarullo, M. R. (2022). Predominio de las cheapfakes en redes sociales: Complejidad técnica y funciones textuales de la desinformación desmentida en Argentina durante 2020.

García-Ull, M. (2021). Deepfakes y responsabilidad penal: desafíos y perspectivas. Revista de Derecho y Tecnología, 8(1), 102-119.

Gómez-Arteta, I., & Escobar-Mamani, F. (2021). Educación virtual en tiempos de pandemia: incremento de la desigualdad social en el Perú. *Revista Chakiñan de Ciencias Sociales y Humanidades*, (15), 152-165.

Goriup, P. D., Haberl, A., Rubel, O., Ajder, V., Kulchytskyy, I., Smaliychuk, A., & Goriup, N. (2019). Potential for renewable use of biomass from reedbeds on the lower Prut, Danube and Dniester floodplains of Ukraine and Moldova. *Mires and Peat*, (25).

Gutiérrez Francés, M. (2002). Las altas tecnologías de la información al servicio del blanqueo de capitales transnacionales. *Delitos financieros, fraude y corrupción en Europa*, 193-214.

Henry, N., Flynn, A., & Powell, A. (2021). The digital abuse of women: Deepfake pornography and the gendered harm of artificial intelligence. Feminist Criminology, 16(1), 3-23. https://doi.org/10.1177/1557085120919697

Johnson, D. G., & Diakopoulos, N. (2021). What to do about deepfakes. Communications of the ACM, 64(3), 33-35.

Marcus, P. (2024, 5 de mayo). Sandra Golpe, Pablo Motos, Resines... Crecen las estafas con 'deep fakes': serán sancionadas hasta con 600.000€. Vozpópuli. https://www.vozpopuli.com/espana/deep-fake-sancion-propuesta-sumar.html

McGuire, M. (2012). Cybercrime: Investigating High-Technology Computer Crime. Pearson.

Pérez Luño, A. E. (1996). Perfiles morales y políticos del derecho a la intimidad. In *Anales de la Real Academia de Ciencias Morales y Políticas* (pp. 311-340). Ministerio de Justicia.

Sinaluisa Sagñay, F. G. ., Romero Noboa, W. P. ., & Freire , N. F. . (2024). Deepfakes Pornográficos: Impacto jurídico-probatorio y social en el Ecuador. Reincisol., 3(6), 2912–2934. https://doi.org/10.59282/reincisol.V3(6)2912-2934

Tiedemann, K. (1996). *Insolvenz-Strafrecht* (pp. 27-y). de Gruyter. https://doi.org/10.1515/9783110899375

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000373434

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.

Wall, D. S., & Williams, M. L. (2013). Policing Cybercrime: Networks and Strategies. Crime Prevention and Community Safety, 15(2), 104–119.

Cerdán Martínez, V. & Padilla Castillo, G. (2019). Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso, en Historia y comunicación social 24 (2), 505-520. https://dx.doi.org/10.5209/hics.66293