Ciencia Digital

www.cienciadigital.org

ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

La responsabilidad penal por el uso de Deep Learning en delitos cometidos contra menores de edad

Criminal liability for the use of Deep Learning in crimes committed against minors

1 Emma Rosa García Delgado https://orcid.org/0009-0000-7887-307X
Universidad Bolivariana del Ecuador (UBE), Durán, Ecuador. Maestría en Derecho Penal
emmagarcia28@yahoo.com

2 Ángela Elizabeth Bustillos Núñez https://orcid.org/0009-0002-7607-0067
Universidad Bolivariana del Ecuador (UBE), Durán, Ecuador.
aebustillosn@ube.edu.ec

3 Sandra Patricia Morejón Llanos https://orcid.org/0009-0009-7229-438X
Universidad Bolivariana del Ecuador (UBE), Durán, Ecuador.
spmorejonl@ube.edu.ec

Artículo de Investigación Científica y Tecnológica

Enviado: 12/01/2026

Revisado: 10/02/2026

Aceptado: 24/03/2026

Publicado: 07/04/2026

DOI: https://doi.org/10.33262/cienciadigital.v10i2.3650

Cítese: García Delgado, E. R., Bustillos Núñez, Ángela E., & Morejón Llanos, S. P. (2026). La responsabilidad penal por el uso de Deep Learning en delitos cometidos contra menores de edad. Ciencia Digital, 10(2), 187-207. https://doi.org/10.33262/cienciadigital.v10i2.3650

CIENCIA DIGITAL, es una revista multidisciplinaria, trimestral, que se publicará en soporte electrónico tiene como misión contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. https://cienciadigital.org

La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec.

Ciencia Digital

ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

www.cienciadigital.org

Palabras claves: Deep Learning generativo, responsabilidad penal, delitos contra menores, evidencia digital sintética, inteligencia artificial, derecho penal tecnológico.

Resumen: Introducción: el desarrollo del Deep Learning generativo introdujo nuevas formas de riesgo en el entorno digital, particularmente en relación con la producción y difusión de contenido sexual sintético que afecta a niños, niñas y adolescentes. Estas tecnologías permiten la creación de representaciones altamente realistas sin necesidad de un hecho material previo, lo que plantea desafíos significativos para la tipificación penal, la imputación de responsabilidad y la valoración probatoria. Objetivos: el presente artículo analiza la responsabilidad penal derivada del uso del Deep Learning en delitos contra menores de edad desde un enfoque jurídico-analítico con base socio-técnica, orientado a evaluar la suficiencia del marco penal ecuatoriano frente a riesgos tecnológicos emergentes. Metodología: a través de un análisis normativo-comparado y del examen crítico de los retos probatorios asociados a la evidencia digital sintética, se identifican vacíos de tipificación y tensiones con los principios de legalidad y culpabilidad. Resultados: Existencia de un vacío normativo en el Ecuador, ineficacia del modelo penal tradicional frente a delitos con IA. Conclusiones: finalmente, se proponen lineamientos normativos y directrices técnicas destinadas a fortalecer una respuesta penal eficaz, garantista y centrada en la protección integral de la niñez frente a los usos ilícitos de la inteligencia artificial. Área de estudio general: Ciencias Sociales. Área de estudio específica: Jurisprudencia. Tipo de artículo: original.

Keywords: Generative deep learning, criminal liability, offenses against minors, synthetic digital evidence, artificial intelligence, technological criminal law.

Introduction: the development of generative Deep Learning introduced new forms of risk in the digital environment, particularly in relation to the production and dissemination of synthetic sexual content that affects children and adolescents. These technologies allow for the creation of highly realistic representations without the need for prior material fact, posing significant challenges for criminalization, attribution of responsibility, and evidentiary assessment. Objectives: this article analyzes the criminal responsibility derived from the use of Deep Learning in crimes against minors from a legal-analytical approach with a socio-technical basis, aimed at evaluating the sufficiency of the Ecuadorian criminal framework in the face of emerging technological risks. Methodology: through a normative-comparative analysis and the critical examination of the evidentiary challenges associated with synthetic digital evidence, typification gaps and

Ciencia Digital
www.cienciadigital.org
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

tensions with the principles of legality and culpability are identified. Results: existence of a regulatory vacuum in Ecuador, ineffectiveness of the traditional penal model against crimes with AI. Conclusions: finally, normative guidelines and technical guidelines are proposed to strengthen an effective, safeguarding criminal response focused on the comprehensive protection of children against the illicit uses of artificial intelligence. General area of study: Social Sciences. Specific area of study: Jurisprudence. Type of item: original.

1. Introducción

El desarrollo y adopción acelerada de sistemas de Inteligencia Artificial (IA) genero transformaciones profundas en los entornos sociales, económicos y jurídicos contemporáneos. En particular, el avance de técnicas basadas en Deep Learning permitió la automatización de procesos complejos de generación de contenido digital, posibilitando la creación de imágenes, audios y videos sintéticos con un alto grado de realismo. Estas capacidades tecnológicas, si bien ofrecen beneficios relevantes en múltiples ámbitos, también incremento exponencialmente los riesgos asociados al uso indebido de la tecnología, especialmente cuando se orienta a la comisión de conductas ilícitas que afectan derechos fundamentales (Sarker, 2021; Ho et al., 2020; Goodfellow et al., 2014).

Uno de los ámbitos más sensibles frente a estas nuevas tecnologías es la protección de niños, niñas y adolescentes en el entorno digital. Diversos informes internacionales advirtieron que la IA generativa está siendo utilizada para producir material sexual infantil sintético, lo que configura una modalidad emergente de explotación sexual en línea. Este tipo de contenido, aun cuando no derive directamente de un abuso físico documentado, produce efectos lesivos significativos sobre la dignidad, la integridad psicológica y el desarrollo integral de las víctimas, agravados por la rápida difusión y persistencia del material en plataformas digitales (*United Nations Interregional Crime and Justice Research Institute* [UNICRI], 2024; *Oficina Europea de Policía* [Europol], 2025; *WeProtect Global Alliance*, 2025).

La problemática del material sexual infantil generado mediante IA fue abordada desde una perspectiva de riesgo global, al evidenciarse que las herramientas de generación sintética reducen las barreras técnicas y económicas para la producción de contenido ilícito. Estudios recientes señalan que esta accesibilidad tecnológica facilito prácticas como la suplantación de identidad, la "nudificación" sintética, la extorsión digital y el grooming automatizado, configurando escenarios delictivos que desafían las categorías tradicionales del derecho penal y del derecho procesal penal (Internet Watch Foundation, 2024; National Center for Missing &

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

Exploited Children, 2025).

¿Desde el punto de vista jurídico-penal, el uso del Deep Learning en delitos contra menores plantea tensiones relevantes entre la necesidad de una tutela reforzada de bienes jurídicos especialmente protegidos y el respeto a los principios estructurales del derecho penal, tales como la legalidad, la tipicidad estricta y la culpabilidad. La doctrina penal contemporánea señalo que los sistemas normativos diseñados para conductas materiales tradicionales presentan dificultades para responder adecuadamente a riesgos derivados de tecnologías altamente automatizadas y desmaterializadas, lo que puede generar tanto lagunas de punibilidad como respuestas normativas desproporcionadas en contextos de criminalidad tecnológica avanzada (Silva, 2011; Brownsword, 2022; Hildebrandt, 2020).

En el contexto ecuatoriano, esta tensión se manifiesta de forma particular. Si bien el ordenamiento jurídico reconoce la protección prioritaria de los derechos de niños, niñas y adolescentes, y contempla tipos penales relacionados con delitos sexuales y delitos informáticos, el Código Orgánico Integral Penal no regula de manera expresa las conductas vinculadas a la producción, posesión o difusión de contenido sexual infantil generado mediante inteligencia artificial. Esta ausencia normativa dificulta la imputación clara de responsabilidades penales y genera incertidumbre en la valoración de la conducta y del daño jurídico producido (Asamblea Nacional del Ecuador, 2014).

A ello se añaden los desafíos probatorios propios del contenido digital sintético. La evidencia generada o manipulada mediante sistemas de IA presenta problemas específicos relacionados con la autenticidad, la integridad y la trazabilidad de los archivos digitales. La literatura especializada en informática forense y gestión de evidencia digital subraya que, sin protocolos adecuados de preservación, cadena de custodia y análisis pericial especializado, existe un alto riesgo de impunidad o de decisiones judiciales basadas en pruebas técnicamente débiles (International Organization for Standardization [ISO], 2012; Casey, 2011).

En respuesta a estos desafíos, distintos organismos internacionales promovieron marcos regulatorios y de gobernanza de la inteligencia artificial basados en el enfoque de riesgos y en la protección de derechos humanos, con especial atención a los grupos en situación de vulnerabilidad, como los menores de edad. Instrumentos como las recomendaciones de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2024), los principios de la Organización para la Cooperación y el Desarrollo Económicos (OECD, 2019) y los marcos de gestión de riesgos del National Institute of Standards and Technology (NIST, 2023) ofrecen criterios relevantes para orientar reformas normativas y fortalecer la respuesta institucional frente a los usos ilícitos de la IA, sin criminalizar la tecnología en abstracto.

En este marco, el presente artículo tiene como objetivo analizar la responsabilidad pe-

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

nal derivada del uso del Deep Learning generativo en delitos cometidos contra menores de edad, a partir de un enfoque jurídico-analítico orientado a evaluar la suficiencia del marco penal ecuatoriano frente a riesgos tecnológicos emergentes. El estudio examina críticamente los vacíos de tipificación y los desafíos probatorios asociados a la evidencia digital sintética, integrando un análisis normativo-comparado y una aproximación socio-técnica que permite contextualizar la interacción entre inteligencia artificial y derecho penal. Con base en este enfoque, se formulan propuestas normativas y directrices técnicas dirigidas a fortalecer una respuesta penal eficaz, garantista y centrada en la protección integral de niños, niñas y adolescentes frente a los usos ilícitos de la inteligencia artificial.

2. Metodología

La investigación se desarrolla a partir de un enfoque cualitativo jurídico, orientado al análisis crítico de la responsabilidad penal en contextos tecnológicos complejos. Este enfoque resulta particularmente adecuado para el estudio de fenómenos normativos emergentes vinculados a la inteligencia artificial, en los que el objeto de análisis no es empírico-estadístico, sino interpretativo, sistemático y valorativo, centrado en la suficiencia del derecho vigente frente a nuevos riesgos sociales (McCrudden, 2019; Banakar & Travers, 2005).

El diseño metodológico se apoya en el método dogmático-jurídico, entendido como una técnica de análisis estructural de normas, principios y categorías jurídicas, que permite examinar la coherencia interna del sistema penal y su capacidad de respuesta frente a conductas no previstas explícitamente por el legislador. Este método resulta idóneo para identificar vacíos de tipificación, problemas de subsunción y tensiones entre innovación tecnológica y principios penales clásicos, sin recurrir a interpretaciones extensivas incompatibles con el principio de legalidad (Hirschl, 2020; Berman, 2011).

De manera complementaria, se utiliza el método de análisis normativo-comparado, con el fin de contrastar el ordenamiento ecuatoriano con desarrollos regulatorios recientes en otros contextos jurídicos. A diferencia del derecho comparado tradicional, este análisis se enfoca en la función regulatoria de la norma frente a riesgos tecnológicos, priorizando instrumentos recientes y experiencias normativas que abordan específicamente la interacción entre inteligencia artificial, protección de menores y responsabilidad penal (De Londras & Mullally, 2020; Brownsword, 2022).

La investigación incorpora, además, un análisis jurídico de base socio-técnica, que permite contextualizar el fenómeno del Deep Learning generativo sin convertir el estudio en un trabajo técnico. Este enfoque reconoce que las normas jurídicas operan sobre infraestructuras digitales concretas y que su eficacia depende de una comprensión mínima de los procesos tecnológicos subyacentes, especialmente cuando estos influyen en la producción de prueba, la atribución de responsabilidad y la valoración del daño

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

jurídico (Yeung, 2018; Hildebrandt, 2020).

Desde el punto de vista analítico, la investigación se estructura en tres momentos: (i) un análisis descriptivo-conceptual, destinado a delimitar el fenómeno del Deep Learning generativo en su dimensión jurídicamente relevante; (ii) un análisis crítico-normativo, orientado a evaluar la suficiencia del marco penal ecuatoriano frente a estos riesgos; y (iii) un análisis propositivo, dirigido a la formulación de reformas normativas y directrices técnicas. Esta secuencia metodológica permite articular de manera coherente el diagnóstico jurídico con las propuestas formuladas en el trabajo (Brownsword, 2022).

3. Resultados

El actual sistema ecuatoriano no puede atribuir responsabilidad de forma eficaz, lo que abre espacios de impunidad. El Ecuador no solo tiene un vacio, sino un retraso normativo frente a estándares internacionales, lo cual establece una omisión normativa que limita la respuesta penal.

3.1 Deep Learning generativo y creación de contenido sintético

Desde el enfoque jurídico-analítico y sociotécnico adoptado en esta investigación, los delitos cometidos mediante tecnologías de Deep Learning generativo plantean retos probatorios y procesales sustanciales para el sistema penal contemporáneo, especialmente cuando involucran a menores de edad. La literatura reciente coincide en que la naturaleza sintética, automatizada y altamente replicable de este tipo de contenido desborda los esquemas tradicionales de investigación penal y exige la actualización de los criterios de obtención, preservación y valoración de la evidencia digital (Verdoliva, 2020; Mirsky & Lee, 2021).

Uno de los principales desafíos se relaciona con la identificación y preservación de la evidencia digital sintética. El contenido generado mediante inteligencia artificial puede carecer de un "original" claramente identificable y puede ser modificado o redistribuido sin pérdida apreciable de calidad, lo que incrementa el riesgo de contaminación probatoria. Estudios recientes subrayan la necesidad de aplicar protocolos de preservación temprana orientados a garantizar la integridad técnica del material digital, la conservación de metadatos relevantes y la trazabilidad de los archivos durante todo el proceso investigativo (NIST, 2023; Verdoliva, 2020).

La cadena de custodia digital, en este contexto, adquiere una dimensión reforzada. La ausencia de mecanismos claros de verificación de integridad y continuidad puede comprometer seriamente la admisibilidad y la fuerza probatoria del contenido sintético en sede judicial. Desde una perspectiva procesal actualizada, se destaca la importancia de incorporar herramientas de verificación técnica y registros documentales que permitan demostrar que la evidencia no fue alterada desde su obtención hasta su valoración judicial (NIST, 2023; Mirsky & Lee, 2021).

Otro reto relevante se presenta en el ámbito de la pericia especializada en detección de

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

contenido generado por inteligencia artificial. La rápida evolución de los modelos generativos genero una brecha constante entre las capacidades de generación y las herramientas de detección disponibles. Investigaciones recientes advierten que los informes periciales deben explicitar de forma transparente sus metodologías, márgenes de error y limitaciones técnicas, evitando conclusiones categóricas que no puedan ser adecuadamente contrastadas en juicio (Tolosana et al., 2020; Köbis et al., 2021).

Desde el punto de vista procesal, la complejidad técnica de este tipo de evidencia plantea interrogantes sobre el equilibrio entre la autoridad técnica del perito y la función valorativa del juez. La doctrina contemporánea señalo que la opacidad algorítmica y la especialización técnica pueden generar una dependencia excesiva del criterio pericial, por lo que resulta indispensable fortalecer la capacitación técnica básica de los operadores de justicia para garantizar una valoración probatoria crítica, razonada y respetuosa del principio de contradicción (Chesney & Citron, 2019; Floridi et al., 2018).

Asimismo, los delitos mediados por Deep Learning presentan con frecuencia una dimensión transnacional, derivada del uso de plataformas digitales globales y servicios de computación en la nube. Informes recientes advierten que la lentitud en la cooperación internacional y la falta de mecanismos eficaces de preservación urgente de datos constituyen obstáculos relevantes para la persecución penal de estas conductas, particularmente en casos de explotación sexual infantil en línea (Europol, 2025; UNICRI, 2024).

En los procesos que involucran a menores de edad, estos retos probatorios deben abordarse desde un enfoque de protección reforzada, orientado a minimizar la revictimización durante la investigación y el juzgamiento. La literatura especializada destaca la necesidad de limitar la exposición innecesaria de las víctimas al contenido ilícito, así como de adoptar técnicas procesales sensibles al impacto psicológico del proceso penal, sin menoscabar el derecho de defensa ni las garantías del imputado (WeProtect Global Alliance, 2025).

3.2 Marco jurídico ecuatoriano y vacíos de tipificación frente a Deep Learning

El ordenamiento jurídico ecuatoriano reconoce una protección reforzada de los derechos de niños, niñas y adolescentes, especialmente frente a toda forma de violencia, explotación y vulneración de su dignidad, incluidas aquellas que se manifiestan en entornos digitales. Este mandato se fundamenta en la Constitución de la República y se articula con obligaciones internacionales asumidas por el Estado en materia de derechos humanos y protección de la infancia, que exigen respuestas normativas eficaces frente a riesgos tecnológicos emergentes (Asamblea Nacional del Ecuador, 2014; Consejo de Europa, 2024).

En el ámbito penal, el Código Orgánico Integral Penal tipifica delitos relacionados con la explotación sexual infantil, la pornografía y determinadas conductas informáticas (Asamblea Nacional del Ecuador, 2014).

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

Sin embargo, estas disposiciones fueron diseñadas bajo un paradigma tecnológico previo al desarrollo masivo de la inteligencia artificial generativa, lo que genera dificultades sustantivas para su aplicación a escenarios en los que el daño se produce mediante representaciones sintéticas creadas algorítmicamente, sin un hecho material previo que sirva de referencia probatoria directa (UNICRI, 2024; Europol, 2025).

Uno de los principales vacíos del marco penal ecuatoriano radica en la ausencia de una tipificación expresa de conductas vinculadas a la producción, posesión y difusión de material sexual infantil sintético. Informes recientes advirtieron que la IA generativa permite crear imágenes y videos sexualizados de menores a partir de datos mínimos, incluso sin contacto directo con la víctima, lo que dificulta la persecución penal cuando los tipos existentes exigen la constatación de un acto material tradicional (*Internet Watch Foundation*, 2024; *WeProtect Global Alliance*, 2025).

Asimismo, el marco jurídico ecuatoriano carece de disposiciones específicas que aborden prácticas emergentes como la suplantación biométrica mediante Deep Learning, la "nudificación" sintética o el uso de agentes conversacionales automatizados para el grooming digital. Estas conductas fueron identificadas a nivel internacional como amenazas crecientes para la seguridad y el desarrollo integral de los menores, y motivaron reformas normativas recientes en otros ordenamientos, basadas en el enfoque de riesgo tecnológico y la protección reforzada de la infancia (*European Parliament & Council of the European Union*, 2024; *Department for Science, Innovation & Technology*, 2025).

En el plano complementario, la Ley Orgánica de Protección de Datos Personales introduce principios relevantes para el tratamiento de datos sensibles, incluidos datos biométricos e imágenes de menores de edad, tales como licitud, minimización y seguridad (Asamblea Nacional del Ecuador, 2021). No obstante, su alcance es predominantemente administrativo y preventivo, por lo que resulta insuficiente para abordar las consecuencias penales derivadas del uso del Deep Learning con fines de explotación sexual infantil. Esta fragmentación normativa evidencia la necesidad de una articulación más coherente entre la protección de datos, la regulación de la inteligencia artificial y el derecho penal sustantivo (Reglamento general a la Ley Orgánica de Protección de Datos Personales) (Presidencia de la República del Ecuador, 2023).

El derecho comparado muestra una tendencia clara hacia la actualización de los marcos penales frente a estos riesgos. Instrumentos recientes, como el Reglamento de Inteligencia Artificial de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 2024) identificaron como prácticas de alto riesgo aquellas que explotan vulnerabilidades relacionadas con la edad, e impulsaron obligaciones reforzadas de prevención, supervisión y responsabilidad. Aunque estas normas no sustituyen al derecho penal interno, ofrecen criterios relevantes pa-

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

ra orientar reformas legislativas compatibles con los principios de legalidad y proporcionalidad (*European Parliament & Council of the European Union*, 2024; *Consejo de Europa*, 2024).

En consecuencia, el marco jurídico ecuatoriano presenta un desfase normativo significativo frente a las nuevas modalidades delictivas mediadas por inteligencia artificial generativa. La ausencia de tipificaciones específicas y de agravantes vinculadas al uso de Deep Learning limita la eficacia de la respuesta penal y dificulta la protección integral de los menores en el entorno digital. Este escenario justifica la necesidad de reformas legislativas actualizadas, basadas en evidencia internacional reciente y en un enfoque de riesgo, que permitan cerrar los vacíos existentes sin comprometer las garantías fundamentales del derecho penal.

3.3 Imputación y responsabilidad penal en delitos mediados por Deep Learning

La imputación de responsabilidad penal en delitos mediados por tecnologías de Deep Learning requiere adaptar las categorías tradicionales del derecho penal a escenarios caracterizados por la automatización, la desmaterialización de la conducta y la intermediación tecnológica. A diferencia de los delitos informáticos clásicos, en los que el autor mantiene un control directo sobre la acción, los sistemas de inteligencia artificial introducen cadenas de intervención más complejas, en las que participan usuarios, desarrolladores, proveedores de servicios y plataformas digitales, lo que obliga a redefinir los criterios de atribución penal de forma compatible con los principios de legalidad y culpabilidad (Brundage et al., 2018; Saltelli & Funtowicz, 2004).

Desde un enfoque contemporáneo de gestión del riesgo, la imputación penal puede fundarse en la creación, incremento o tolerancia de riesgos tecnológicamente relevantes que se materializan en la lesión de bienes jurídicos especialmente protegidos, como la indemnidad sexual y la dignidad de los menores de edad. En este sentido, el uso deliberado de herramientas de Deep Learning para generar o difundir material sexual infantil sintético constituye un supuesto claro de asunción consciente del riesgo, mientras que la facilitación negligente de estas tecnologías puede dar lugar a formas de responsabilidad por imprudencia grave, cuando el resultado era objetivamente previsible (Saltelli & Funtowicz, 2004; Floridi et al., 2018).

El análisis del elemento subjetivo adquiere particular relevancia en contextos de inteligencia artificial generativa. La literatura reciente señalo que el dolo puede configurarse no solo a partir de la intención directa de producir el resultado, sino también mediante la aceptación consciente de los efectos potencialmente lesivos del uso de sistemas generativos en entornos de alto riesgo. En delitos contra menores, la previsibilidad del daño y el conocimiento generalizado sobre los usos ilícitos de estas tecnologías refuerzan la posibilidad de apreciar dolo eventual o, en su defecto, imprudencia penalmente relevante (Cheng et al., 2017; Brundage et

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

al., 2018).

La responsabilidad penal de actores intermedios como desarrolladores de software, proveedores de servicios de alojamiento o plataformas digitales se convirtió en uno de los aspectos más debatidos en la doctrina reciente. En estos supuestos, la imputación no se basa en la autoría directa del contenido ilícito, sino en la omisión de deberes razonables de prevención, supervisión o retirada, especialmente cuando estos actores tienen capacidad técnica y organizativa para mitigar el riesgo. Este enfoque se vincula con modelos de responsabilidad por omisión impropia y con la noción de posiciones de garantía derivadas del control de infraestructuras digitales de alto impacto (*European Parliament & Council of the European Union*, 2024; *Council of Europe*, 2024).

Asimismo, la responsabilidad penal de las personas jurídicas adquiere una dimensión central en los delitos mediados por inteligencia artificial. La doctrina contemporánea sostiene que las organizaciones pueden ser penalmente responsables cuando la comisión del delito revela fallas estructurales en los sistemas de cumplimiento, ausencia de evaluaciones de riesgo o incentivos económicos que favorecen la tolerancia de conductas ilícitas. En el contexto del Deep Learning, la falta de mecanismos de control, auditoría y trazabilidad puede constituir un indicio relevante de negligencia organizacional penalmente imputable (Nieto, 2013; NIST, 2023).

En el ámbito específico de la protección de menores, los estándares internacionales recientes enfatizan la necesidad de aplicar un estándar reforzado de diligencia a todos los actores que operan tecnologías con potencial de daño significativo. Este enfoque no implica una criminalización general de la innovación, sino la exigencia de medidas proporcionales de prevención y control en actividades consideradas de alto riesgo. La imputación penal, en estos casos, debe articularse de manera cuidadosa para sancionar conductas verdaderamente reprochables sin erosionar las garantías fundamentales del derecho penal (*WeProtect Global Alliance*, 2025; UNICRI, 2024).

3.4 Retos probatorios y procesales: evidencia digital y contenido sintético

La incorporación de tecnologías de Deep Learning en la comisión de delitos contra menores de edad introduce retos probatorios sustanciales para el proceso penal, especialmente en lo relativo a la obtención, preservación, análisis y valoración de la evidencia digital. A diferencia de los medios probatorios tradicionales, el contenido sintético generado por inteligencia artificial presenta características técnicas que dificultan la determinación de su origen, autenticidad e integridad, lo que exige una adaptación de los estándares procesales y periciales vigentes (Verdoliva, 2020; Mirsky & Lee, 2021).

Uno de los principales desafíos radica en la identificación y preservación de la evidencia digital. Los archivos audiovisuales sintéticos pueden ser copiados, modificados o redistribuidos sin pérdida apreciable de

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

calidad, lo que incrementa el riesgo de alteración probatoria. Por ello, la literatura especializada subraya la necesidad de aplicar protocolos estrictos de preservación temprana, que incluyan la conservación de metadatos, el aseguramiento de dispositivos y la documentación exhaustiva de cada etapa del proceso de recolección, conforme a estándares internacionales de informática forense (Kent et al., 2006; ISO, 2012).

En los casos de contenido generado mediante Deep Learning, la cadena de custodia digital adquiere un valor central. La ausencia de registros claros sobre el origen del archivo, las herramientas utilizadas o las modificaciones realizadas puede comprometer la admisibilidad de la prueba o debilitar su fuerza probatoria en juicio. En este contexto, los lineamientos técnicos recomiendan el uso de mecanismos de sellado criptográfico, registros de integridad y procedimientos reproducibles que permitan verificar que la evidencia no fue alterada desde su incautación hasta su presentación en sede judicial (Casey, 2011; ISO, 2012).

Otro reto relevante es la pericia especializada en detección de contenido sintético. Si bien existen técnicas forenses orientadas a identificar patrones de manipulación o generación algorítmica, la rápida evolución de los modelos generativos produce una brecha constante entre las capacidades de generación y las herramientas de detección. Esta asimetría tecnológica implica que los informes periciales deben explicitar de manera transparente sus márgenes de error, limitaciones metodológicas y niveles de confianza, a fin de evitar conclusiones categóricas no sustentadas científicamente (Rössler et al., 2019; Tolosana et al., 2020).

Desde el punto de vista procesal, la valoración de este tipo de evidencia plantea interrogantes sobre los criterios de confiabilidad y suficiencia probatoria. Diversos autores advirtieron que la complejidad técnica de los algoritmos puede generar una dependencia excesiva del criterio pericial, desplazando indebidamente la función valorativa del juez. Frente a ello se propuso reforzar la capacitación de operadores de justicia y establecer pautas claras para la evaluación crítica de la prueba pericial en casos que involucren inteligencia artificial (Chesney & Citron, 2019; Floridi et al., 2018).

Adicionalmente, los delitos mediatos por Deep Learning suelen presentar una dimensión transnacional, debido al uso de plataformas globales, servicios en la nube y redes descentralizadas. Esta característica dificulta la obtención oportuna de información relevante, como registros de acceso, direcciones IP o datos de usuarios, y exige mecanismos ágiles de cooperación internacional y conservación urgente de datos. Organismos internacionales señalaron que la falta de coordinación entre autoridades y plataformas tecnológicas constituye uno de los principales obstáculos para la persecución penal efectiva de estos delitos (Europol, 2025; UNICRI, 2024).

En el caso específico de delitos contra menores, los retos probatorios deben analizarse desde un enfoque de protección reforzada,

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

que priorice la minimización de la revictimización durante el proceso penal. Ello implica adoptar medidas procesales que eviten la exposición innecesaria de la víctima al contenido ilícito, así como el uso de técnicas probatorias que reduzcan el impacto psicológico del proceso judicial, sin menoscabar el derecho de defensa ni el principio de contradicción (WeProtect Global Alliance, 2025; Consejo de Europa, 2024).

3.5 Derecho comparado y estándares internacionales

El análisis comparado constituye una herramienta clave para abordar los desafíos que plantea el uso del Deep Learning generativo en delitos contra menores de edad, en la medida en que permite identificar tendencias regulatorias emergentes, buenas prácticas normativas y criterios interpretativos que pueden orientar reformas internas. En los últimos años, diversos ordenamientos y organismos internacionales reconocieron que la inteligencia artificial genera riesgos específicos para la infancia, lo que impulso respuestas normativas basadas en la protección reforzada y en el enfoque de riesgo tecnológico (OECD, 2019; UNESCO, 2024).

En el ámbito europeo, la adopción del Reglamento de Inteligencia Artificial de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 2024) (AI Act) representa uno de los desarrollos normativos más relevantes. Este instrumento establece un sistema de clasificación de riesgos y prohíbe prácticas que explotan vulnerabilidades relacionadas con la edad, además de imponer obligaciones reforzadas para sistemas considerados de alto riesgo. Si bien el AI Act no es una norma penal en sentido estricto, su enfoque resulta especialmente relevante para los delitos contra menores, al identificar usos de la IA que requieren controles estrictos, supervisión humana y mecanismos de rendición de cuentas (*European Parliament & Council of the European Union*, 2024).

De manera complementaria, el Consejo de Europa (2024) promovió un marco jurídico orientado a garantizar la compatibilidad de los sistemas de inteligencia artificial con los derechos humanos, la democracia y el Estado de derecho. La Convención Marco sobre Inteligencia Artificial y Derechos Humanos (Council of Europe, 2024). subraya la obligación de los Estados de prevenir daños significativos derivados del uso de tecnologías automatizadas, con especial atención a los grupos en situación de vulnerabilidad, como los niños, niñas y adolescentes. Este enfoque refuerza la necesidad de integrar estándares de protección infantil en las respuestas penales y procesales frente al uso ilícito de la IA.

En el contexto anglosajón, el Reino Unido avanzo en el reconocimiento explícito del material de abuso sexual infantil generado por inteligencia artificial como una amenaza creciente. Informes gubernamentales recientes y reformas legislativas enfatizaron la persecución penal de la creación de imágenes sexuales sintéticas de menores “en la fuente”, es decir, antes de su difusión masiva, destacando la necesidad de criminalizar

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

estas conductas incluso cuando no exista una víctima identificable en un hecho real previo (*Department for Science, Innovation & Technology*, 2025).

A nivel internacional, organismos especializados alertaron de manera reiterada sobre el impacto de la inteligencia artificial generativa en la explotación sexual infantil en línea. La Oficina de las Naciones Unidas contra la Droga y el Delito y el UNICRI (2024) señalaron que la IA amplifica la escala y la sofisticación de estas conductas, dificultando la detección y persecución penal. En respuesta se recomendó marcos normativos integrales que combinen tipificación penal específica, cooperación internacional y fortalecimiento de capacidades técnicas en las agencias de justicia (UNICRI, 2024).

Por su parte, iniciativas multilaterales como *WeProtect Global Alliance* (2025) y los reportes estratégicos de Europol (2025) puso énfasis en la necesidad de respuestas coordinadas entre Estados, plataformas digitales y proveedores tecnológicos. Estos organismos destacan que la persecución penal aislada resulta insuficiente frente a delitos transnacionales mediados por inteligencia artificial, y proponen modelos de gobernanza que integren prevención, detección temprana, preservación de evidencia digital y protección centrada en la víctima.

Asimismo, los marcos de gobernanza y gestión de riesgos de la inteligencia artificial, como los desarrollados por el NIST (2023) aportan criterios técnicos relevantes para el ámbito penal. Aunque estos instrumentos no tienen carácter sancionador, ofrecen estándares sobre evaluación de riesgos, trazabilidad, transparencia y responsabilidad organizacional que pueden ser incorporados como referencias técnicas en investigaciones penales y en la formulación de políticas públicas orientadas a la protección de menores frente a usos ilícitos de la IA (NIST, 2023).

En conjunto, el derecho comparado y los estándares internacionales evidencian una convergencia hacia modelos normativos que reconocen el carácter altamente riesgoso del uso de inteligencia artificial generativa en contextos que involucran a menores de edad. Estas experiencias muestran que una respuesta eficaz no depende exclusivamente de la expansión del derecho penal, sino de la articulación entre tipificación precisa, obligaciones preventivas, cooperación internacional y fortalecimiento de capacidades técnicas. Para el caso ecuatoriano, estos desarrollos ofrecen insumos valiosos para diseñar reformas coherentes con las tendencias globales y con los principios fundamentales del derecho penal.

3.6 Propuesta de reformas normativas y directrices técnicas para Ecuador

El análisis previo evidencia que el ordenamiento jurídico ecuatoriano presenta un desfase significativo frente a las nuevas modalidades delictivas mediadas por tecnologías de Deep Learning generativo, especialmente cuando estas afectan a niños, niñas y adolescentes. En este contexto, resulta necesario proponer un conjunto de reformas normati-

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

vas y directrices técnicas que permitan fortalecer la tutela penal sin comprometer los principios fundamentales del derecho penal ni obstaculizar el desarrollo legítimo de la innovación tecnológica.

En el plano del derecho penal sustantivo, se propone la incorporación de una tipificación específica de las conductas relacionadas con la producción, posesión y difusión de material sexual infantil generado mediante inteligencia artificial. Esta figura penal debería describir de forma expresa la creación de representaciones sintéticas sexualizadas de menores, independientemente de la existencia de un hecho material real previo, atendiendo al daño jurídico que produce la representación y su circulación. La experiencia comparada demuestra que la claridad típica es esencial para evitar vacíos de punibilidad y garantizar el respeto al principio de legalidad (UNICRI, 2024; *Department for Science, Innovation & Technology*, 2025).

De manera complementaria, se recomienda incorporar una agravante específica para los delitos contra la integridad sexual, la intimidad y la identidad personal cuando se empleen herramientas de Deep Learning u otros sistemas de inteligencia artificial generativa. Esta agravante permitiría reflejar el mayor grado de reproche asociado a la sofisticación tecnológica, la facilidad de difusión masiva y la persistencia del daño en entornos digitales, sin necesidad de crear tipos penales excesivamente fragmentados (*European Parliament & Council of the European Union*, 2024; **WeProtect Global Alliance**, 2025).

En relación con la responsabilidad penal de personas jurídicas, se sugiere reforzar las disposiciones existentes para contemplar de manera expresa la obligación de implementar sistemas de gestión del riesgo tecnológico en organizaciones que desarrollen, operen o faciliten tecnologías de alto impacto. La ausencia de evaluaciones de riesgo, mecanismos de control interno, auditorías técnicas o canales eficaces de denuncia debería considerarse un indicio relevante de negligencia organizacional penalmente imputable, en consonancia con los enfoques contemporáneos de gobernanza de la inteligencia artificial (NIST, 2023; OECD, 2019).

Desde la perspectiva procesal y probatoria, se propone la adopción de reglas mínimas para la preservación y análisis de evidencia digital en casos que involucren contenido sintético. Estas reglas deberían incluir la conservación temprana de metadatos, el uso de sellos de integridad criptográfica, la documentación exhaustiva de la cadena de custodia digital y la estandarización de criterios para la pericia en detección de contenido generado por IA. La incorporación de estos lineamientos fortalecería la confiabilidad de la prueba y reduciría el riesgo de impunidad por deficiencias técnicas (ISO, 2012; Kent et al., 2006; NIST, 2023).

Asimismo, resulta recomendable el desarrollo de protocolos especializados de actuación para fiscales, jueces y peritos en casos de delitos contra menores mediados por inteligencia artificial. Estos protocolos deberían contemplar medidas orientadas a minimizar la revictimización, limitar la ex-

Ciencia Digital
www.cienciadigital.org
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

posición innecesaria al contenido ilícito y garantizar un enfoque centrado en los derechos de la niñez, sin menoscabar el derecho de defensa ni el principio de contradicción. La capacitación técnica continua de los operadores de justicia constituye un elemento indispensable para la aplicación efectiva de estas directrices (Consejo de Europa, 2024; *WeProtect Global Alliance*, 2025).

En el ámbito de la cooperación interinstitucional e internacional, se propone fortalecer los mecanismos de preservación urgente de datos y de intercambio de información con plataformas digitales y autoridades extranjeras. Dada la naturaleza transnacional de los delitos mediados por Deep Learning, la eficacia de la persecución penal depende en gran medida de la rapidez en la obtención de registros técnicos y de la coordinación entre actores públicos y privados. Las experiencias internacionales muestran que la falta de cooperación temprana constituye uno de los principales obstáculos para la protección efectiva de menores en el entorno digital (Europol, 2025; UNICRI, 2024).

4. Discusión

Los hallazgos de este estudio confirman que el uso del Deep Learning generativo en delitos cometidos contra menores de edad representa un desafío estructural para los sistemas penales contemporáneos, coincidiendo con la literatura reciente que advierte sobre la insuficiencia de los marcos normativos tradicionales frente a tecnologías altamente automatizadas y desmaterializadas (UNICRI, 2024; Europol, 2025). En particular, la posibilidad de generar contenido sexual infantil sintético sin un hecho material previo refuerza la necesidad de repensar los criterios de tipificación penal desde una lógica centrada en el daño jurídico y no exclusivamente en la materialidad de la conducta.

En este sentido, los vacíos identificados en el ordenamiento jurídico ecuatoriano se alinean con problemáticas detectadas en otros contextos nacionales, donde la falta de regulación específica dificulto la persecución penal efectiva de estas conductas. Estudios comparados muestran que los Estados que avanzaron en la tipificación expresa del material sexual infantil generado por inteligencia artificial logro una mayor claridad en la imputación penal, reduciendo el margen de interpretaciones extensivas incompatibles con el principio de legalidad (*Department for Science, Innovation & Technology*, 2025; *European Parliament & Council of the European Union*, 2024).

Asimismo, el análisis de la responsabilidad penal revela que los enfoques contemporáneos basados en la gestión del riesgo tecnológico ofrecen una alternativa sólida frente a los modelos puramente reactivos del derecho penal clásico. La literatura especializada sostiene que la imputación diferenciada de responsabilidades entre usuarios finales, actores intermedios y personas jurídicas permite una respuesta más proporcional y eficaz, especialmente cuando se trata de entornos digitales de alto riesgo para menores de edad (Brundage et al., 2018; NIST, 2023; *WeProtect Global Alliance*, 2025).

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

En el ámbito probatorio, los resultados obtenidos refuerzan las advertencias formuladas por organismos técnicos y académicos sobre la fragilidad de la evidencia digital sintética si no se aplican protocolos rigurosos de preservación y análisis. La dependencia excesiva de pericias opacas o no reproducibles identificadas como un factor de riesgo para la validez del proceso penal, lo que coincide con los estándares internacionales que recomiendan transparencia metodológica, documentación exhaustiva y explicitación de márgenes de error en los informes periciales (ISO, 2012; Kent et al., 2006; Mirsky & Lee, 2021).

El derecho comparado y los estándares internacionales analizados respaldan las propuestas formuladas en este artículo, al evidenciar una convergencia hacia modelos normativos que priorizan la protección reforzada de la infancia y la prevención de daños derivados del uso indebido de la inteligencia artificial. Tanto los marcos regulatorios europeos como los informes de organismos multilaterales subrayan que la respuesta penal aislada resulta insuficiente si no se articula con mecanismos de cooperación internacional, gobernanza tecnológica y obligaciones preventivas para los actores privados involucrados (Consejo de Europa, 2024; OECD, 2019; UNICRI, 2024).

5. Conclusiones

- El desarrollo del Deep Learning generativo transformo de manera sustancial los escenarios de riesgo asociados a los delitos cometidos contra menores de edad, al permitir la creación y difusión de contenido sintético altamente realista con capacidad de causar daños graves y persistentes. Este fenómeno evidencia que las tecnologías de inteligencia artificial no solo amplifican conductas delictivas preexistentes, sino que también generan nuevas formas de agresión digital que desafían las categorías tradicionales del derecho penal.
- El análisis realizado demuestra que el ordenamiento jurídico ecuatoriano presenta vacíos relevantes frente a estas nuevas modalidades delictivas, especialmente en lo relativo a la tipificación expresa de la producción, posesión y difusión de material sexual infantil generado mediante inteligencia artificial. La ausencia de figuras penales específicas y de agravantes vinculadas al uso de tecnologías generativas dificulta la persecución penal efectiva y genera incertidumbre en la imputación de responsabilidades.
- Asimismo, se concluye que la responsabilidad penal en delitos mediados por Deep Learning no puede limitarse al autor material del contenido ilícito, sino que debe considerar, de manera diferenciada y garantista, la participación de actores intermedios y personas jurídicas cuando exista control del riesgo, capacidad de prevención y omisión de deberes razonables de diligencia. Este enfoque permite evitar tanto la impunidad como la expansión desproporcionada del ius puniendi.

Ciencia Digital
ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original
www.cienciadigital.org

- En el ámbito procesal, los retos probatorios asociados a la evidencia digital sintética ponen de manifiesto la necesidad de actualizar los estándares tradicionales de investigación y valoración de la prueba. La preservación adecuada de la evidencia, la cadena de custodia digital, la pericia especializada y la capacitación de los operadores de justicia constituyen elementos indispensables para garantizar procesos penales eficaces y respetuosos de las garantías fundamentales.

- El examen del derecho comparado y de los estándares internacionales confirma que existe una tendencia convergente hacia modelos normativos basados en el enfoque de riesgo y en la protección reforzada de la infancia frente a los usos ilícitos de la inteligencia artificial. Estas experiencias ofrecen insumos valiosos para el diseño de reformas legislativas y políticas públicas adaptadas a la complejidad tecnológica actual, sin criminalizar la innovación legítima.

- La tutela penal efectiva de los derechos de niños, niñas y adolescentes frente a los riesgos derivados del Deep Learning generativo exige una respuesta integral, que combine tipificación penal precisa, fortalecimiento probatorio, responsabilidad diferenciada de los actores involucrados y una gobernanza tecnológica coherente. Solo a través de esta articulación será posible garantizar una protección real y sostenible de la niñez en un entorno digital marcado por la rápida evolución de la inteligencia artificial.

6. Conflicto de intereses

Los autores declaran que no existe conflicto de intereses en relación con el artículo presentado.

7. Declaración de contribución de los autores

Todos autores contribuyeron significativamente en la elaboración del artículo.

8. Costos de financiamiento

La presente investigación fue financiada en su totalidad con fondos propios de los autores.

9. Referencias Bibliográficas

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. Registro Oficial Suplemento No. 180, Ley 0. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento No. 459. hhttps://www.telecomunicaciones.gob.ec/wp-content/uploads

ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

/2021/06/Ley-Organica-de-Datos-Personales.pdf

Banakar, R., & Travers, M. (2005). Theory and method in socio-legal research. Bloomsbury Publishing. https://www.researchgate.net/publication/228262192_Theory_and_Method_in_Socio-Legal_Research

Berman, M. N. (2011). Constitutional Interpretation: Non-originalism. Philosophy Compass, 6(6), 408-420. https://philpapers.org/rec/BERCIN

Brownsword, R. (2022). Law, technology and society: Re-imagining the regulatory environment. Routledge. https://www.routledge.com/Law-Technology-and-Society-Reimagining-the-Regulatory-Environment/Brownsword/p/book/9780815356462

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., . . . Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Apollo - University of Cambridge Repository. https://www.repository.cam.ac.uk/items/d654418d-1c12-4024-85d5-ccd614c32ef3

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press. https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(C):e1211. https://www.researchgate.net/publication/318152978_Enterprise_data_breach_causes_challenges_prevention_and_future_directions_Enterprise_data_breach

Chesney, R., & Citron, D. K. (2019). Deep fakes: a looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1819. https://doi.org/10.15779/Z38RV0D15J

Consejo de Europa. (2024). Framework convention on artificial intelligence and human rights, democracy and the rule of law (CETS No. 225). https://www.coe.int

Council of Europe. (2024). Framework convention on artificial intelligence. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

De Londras, F., & Mullally, S. (2020). Irish yearbook of international law: Volume 13,2018. Hart Publishing. https://research.birmingham.ac.uk/en/publications/irish-yearbook-of-international-law-volume-13-2018/

Department for Science, Innovation & Technology. (2025). New law to tackle AI child

ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

abuse images at source as reports more than double. https://www.gov.uk/government/news/new-law-to-tackle-ai-child-abuse-images-at-source-as-reports-more-than-double

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... Vayena, E. (2018). AI4People-an ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27. https://papers.nips.cc/paper_files/paper/2014/hash/f033ed80deb0234979a61f95710dbe25-Abstract.html

Hildebrandt, M. (2020). Law for computer scientists and other folk. Oxford University Press. https://www.cohubicol.com/assets/uploads/law_for_computer_scientists.pdf

Hirschl, R. (2020). Comparative matters: The renaissance of comparative constitutional law. Oxford University Press. https://www.scjn.gob.mx/relaciones-institucionales/sites/default/files/page/2021-02/Resen%CC%83a_%20Comparative%20Matters%2C%20The%20Renaissance%20of%20Comparative%20Constitutional%20Law.pdf

Ho, J., Jain, A., & Abbeel, P. (2020). Denoising diffusion probabilistic models. Advances in Neural Information Processing Systems. https://arxiv.org/abs/2006.11239

International Organization for Standardization (ISO). (2012). ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence (edition 1). https://www.iso.org/standard/44381.html

Internet Watch Foundation. (2024). Artificial intelligence and child sexual abuse material. https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/ai-generated-child-sexual-abuse/

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST SP 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Köbis, N. C., Doležalová, B., & Soraperra, I. (2021). Fooled twice: people cannot detect deepfakes but think they can. iScience, 24(11), 103364. https://doi.org/10.1016/j.isci.2021.103364

ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

McCrudden, C. (2019). Understanding human dignity. Oxford University Press. https://pure.qub.ac.uk/en/publications/understanding-human-dignity/

Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: a survey. ACM Computing Surveys, 54(1), 1-41. https://doi.org/10.1145/3425780

National Center for Missing & Exploited Children. (2025). Spike in online crimes against children a "wake-up call." https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call

National Institute of Standards and Technology [NIST]. (2023). Artificial intelligence risk management framework (AI RMF 1.0). https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

Nieto Martín, A. (2013). La responsabilidad penal de las personas jurídicas: oportunidades y retos para la cooperación judicial. Armonización penal en Europa. https://dialnet.unirioja.es/servlet/articulo?codigo=6378120

Oficina Europea de Policía [Europol]. (2025). The changing DNA of serious and organized crime: EU serious and organized crime threat assessment (SOCTA 2025). https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2024). Recommendation on the ethics of artificial intelligence. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

Organización para la Cooperación y el Desarrollo Económicos [OECD]. (2019). Recommendation of the council on artificial intelligence. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

Parlamento Europeo y Consejo de la Unión Europea. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Presidencia de la República del Ecuador. (2023). Reglamento general a la Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento No. 435, Norma 904. https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Niessner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. 2019 IEEE/CVF International Conference on Computer Vision (ICCV), 1–11. IEEE.

ISSN: 2602-8085
Vol. 10 No. 2, pp. 187 – 207, abril - junio 2026
Revista Multidisciplinar
Artículo original

https://doi.org/10.1109/ICCV.2019.00009

Saltelli, A., & Funtowicz, S. (2004). The precautionary principle: implications for risk management strategies. International Journal of Occupational Medicine and Environmental Health, 17(1), 47–57. https://pubmed.ncbi.nlm.nih.gov/15212206/

Sarker, I. H. (2021). Deep learning: a comprehensive overview. SN Computer Science, 2(6), 420. https://doi.org/10.1007/s42979-021-00815-1

Silva Sánchez, J. M. (2011). La expansion del derecho penal (2.ª ed.). Civitas. https://es.scribd.com/doc/119471893/La-Expansion-del-Derecho-Penal-Jesus-Silva-Sanchez

Tolosana, R., Vera-Rodríguez, R., Fierrez, J., Morales, A., & Ortega-García, J. (2020). Deepfakes and beyond: a survey. Information Fusion, 64, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

United Nations Interregional Crime and Justice Research Institute [UNICRI]. (2024). Generative AI: a new threat for online child sexual exploitation and abuse. https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf

Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

WeProtect Global Alliance. (2025). Global threat assessment. https://www.weprotect.org/global-threat-assessment-25/

Yeung, K. (2018). Algorithmic regulation: a critical interrogation. Regulation & Governance, 12(4), 505–523. https://doi.org/10.1111/rego.12158