runas
Journal of Education & Culture

# Valoración procesal penal de la pornografía infantil generada por inteligencia artificial en Ecuador

*Procedural criminal law assessment of child pornography generated by artificial intelligence in Ecuador*

**Mateo David Arias Ordóñez, Andrea Lisseth Durán Ramírez**

## Resumen

La presente investigación se centró en analizar la posibilidad legal de aceptar pruebas digitales generadas mediante inteligencia artificial (IA) en el procedimiento penal ecuatoriano, en lo que respecta a la digitalización y producción de material sexual infantil. En los últimos años, el rápido avance de los deepfakes y de los modelos completamente automatizados de generación de imágenes ha transformado de manera sustancial las condiciones en torno a la apreciación de las pruebas judiciales. En la investigación se utilizaron métodos cualitativos, combinando enfoques dogmático-jurídicos, analítico-sintéticos y hermenéuticos. El estudio permitió considerar la legislación ecuatoriana, la doctrina especializada y experiencias comparadas para identificar vacíos legales que dificultan un tratamiento uniforme de la prueba digital. Se verificó que, aunque la normativa ecuatoriana reconoce principios como la legalidad de la prueba, la cadena de custodia y la motivación judicial, aún se carece de normas que permitan autenticar o evaluar archivos generados mediante algoritmos. También se identificó jurisprudencia internacional que subraya la necesidad de controles periciales más rigurosos y mecanismos de autenticidad más sólidos. Finalmente, el trabajo amplía su enfoque hacia los derechos penalmente protegidos que se ven amenazados por la creación de pornografía infantil mediante IA, subrayando que recae sobre el Estado la responsabilidad de garantizar la dignidad, integridad y desarrollo integral de la niñez como eje central de toda respuesta penal.

Palabras clave: Prueba digital; aplicación informática; administración de justicia; derechos del niño; pornografía infantil sintética.

**Mateo David Arias Ordóñez**
Universidad Católica de Cuenca | Cuenca | Ecuador | mateo.arias@est.ucacue.edu.ec
https://orcid.org/0009-0004-4950-2850
**Andrea Lisseth Durán Ramírez**
Universidad Católica de Cuenca | Cuenca | Ecuador | aduranr@ucacue.edu.ec
https://orcid.org/0000-0002-8382-1335

https://doi.org/10.46652/runas.v7i14.329
ISSN 2737-6230
Vol. 7 No. 14 enero-junio 2026, e260329
Quito, Ecuador

Enviado: octubre 21, 2025
Aceptado: diciembre 18, 2025
Publicado: enero 05, 2026
Continuous Publication



RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

## Abstract

This research focuses on analyzing the legal possibility of accepting digital evidence generated by artificial intelligence (AI) in Ecuadorian criminal proceedings, specifically regarding the digitization and production of child sexual abuse material. In recent years, the rapid advancement of deepfakes and fully automated image generation models has substantially transformed the conditions surrounding the evaluation of evidence in court. The research employed qualitative methods, combining dogmatic-legal, analytical-synthetic, and hermeneutical approaches. The study considered Ecuadorian legislation, specialized doctrine, and comparative experiences to identify legal gaps that hinder the uniform treatment of digital evidence. It was found that, although Ecuadorian regulations recognize principles such as the legality of evidence, chain of custody, and judicial reasoning, there are still no rules for authenticating or evaluating files generated by algorithms. International jurisprudence was also identified that underscores the need for more rigorous expert controls and more robust authentication mechanisms. Finally, the work broadens its focus to the criminally protected rights that are threatened by the creation of child pornography through AI, emphasizing that the responsibility to guarantee the dignity, integrity and integral development of children as the central focus of any criminal response falls on the State.

Keywords: Digital evidence; artificial intelligence; administration of justice; children's rights; synthetic child pornography.

## Introducción

La IA comprende un conjunto de programas y sistemas capaces de desarrollar tareas que eran antes exclusivas del razonamiento humano (Russell & Norvig, 2012). Su expansión ha transformado la manera en que se crean, distribuyen y consumen los contenidos digitales, abriendo nuevas oportunidades para la comunicación y la ciencia, pero también escenarios inéditos de riesgo para el derecho penal.

Entre sus manifestaciones más inquietantes destaca la elaboración de material sexual infantil producido digitalmente mediante técnicas de deepfake u otras herramientas. Dichas herramientas pueden generar imágenes o videos que aparentan ser reales sin que haya intervenido ningún menor de edad. Aunque en tales casos no exista una víctima física, el daño simbólico y social es evidente: se banaliza la explotación sexual infantil, se vulnera la dignidad de los niños y se fomenta la circulación de contenidos que pueden inducir a delitos reales.

En Ecuador, el marco jurídico vigente, representado principalmente por el Código Orgánico Integral Penal (COIP), resulta todavía insuficiente frente a esta realidad. Si bien dicha normativa sanciona de manera severa los delitos de explotación sexual infantil, no contempla expresamente los contenidos digitales producidos mediante inteligencia artificial. Además, el proceso penal no dispone aún de parámetros técnicos definidos que orienten la admisibilidad y valoración de este tipo de pruebas digitales.

Como indica Ferrajoli (1995),

> la validez de una prueba no depende solo de su contenido, sino también del modo en que se obtiene y se controla. Esta advertencia cobra particular relevancia cuando la evidencia proviene de sistemas automatizados que pueden ser alterados o manipulados.

En función de lo cual surge la siguiente pregunta como pregunta inicial, ¿Es viable desde un sentido legal, la inclusión de pruebas digitales generadas por la IA, en lo relacionado a los procesos penales, en materia sexual infantil en Ecuador, sin que se comprometa el debido proceso?

Por lo que se trata de aspectos que son abordados en un enfoque práctico, para con ello determinar se es posible introducir estas pruebas sin que implique una vulneración de derechos, dentro de lo que son los principios de garantismo y priorización de la integridad del procedimiento. De manera que, el análisis se centra en dos fundamentales aspectos, por una parte, la normativa, tanto nacional, como internacionales, y por la otra, lo referente a los riesgos procesales propios de la prueba digital, que implican la autenticidad, las posibles manipulaciones, y los obstáculos en lo referente al ejercicio de la contradicción.

Por lo cual, se buscó la comprensión de los elementos que afectan, la práctica, el funcionamiento de la justicia penal y la prevalencia de las garantías esenciales, en los avances de las tecnologías. En referencias a ello Muñoz (2015), destaca: que toda prueba debe ser valorado en base a la presunción inocencia y del principio de contradicción, por lo que la adopción de las TICs, no puede condicionar la aplicación de tales principios.

En función de lo cual, el estudio se fundamenta, en los elementos relativos a la aceptación de las pruebas digitales generadas por la IA puede ser válido legalmente, basado consecuentemente en controles reales y verificables. Para lo que debe primar estándar técnico, y peritajes. Al igual que la formación especializada en la materia a fiscales y defensores (Loreti, 2020).

En resumen, este trabajo busca contribuir al diseño de un modelo procesal penal ecuatoriano que integre tecnología e institucionalidad sin sacrificar la esencia garantista del debido proceso. El propósito es que el sistema de justicia disponga de herramientas normativas y técnicas capaces de responder a los desafíos de la era digital, preservando la protección integral de la niñez.

## Marco teórico

### *Principales herramientas de inteligencia artificial utilizadas para generar pornografía infantil sintética*

El fenómeno de la pornografía infantil generada mediante inteligencia artificial (IA) trasciende ampliamente los conocidos deepfakes. Hoy existen múltiples herramientas capaces de crear material sexual sin la participación de menores reales, lo que incrementa la complejidad del control judicial y de la valoración probatoria. Comprender estas modalidades resulta indispensable para adaptar las respuestas procesales a los nuevos riesgos tecnológicos.

En primer lugar, destacan los modelos generativos de texto a imagen, como Stable Diffusion, Midjourney o DALL·E, que permiten crear ilustraciones a partir de simples descripciones escritas. Son TICs que pueden ser usadas en usos ilícitos, mostrando escenas sexuales que involucren a

los menores, en el que son generadas imágenes con apariencias realistas y difíciles de rastrear. La autenticidad digital se garantiza por meta-datos demostrables (Lynch, 2000).

En segundo lugar, las aplicaciones de nudify o "desnudo sintético, son creados a partir de programas que se alteran de manera digital o modifican imágenes que son reales. La cuestión es conseguir resultados realistas que dan la percepción de ser legítimos. Cuestión que remarca la importancia de contar con adecuados peritajes en informática, dentro del derecho penal (Casey, 2019).

Finalmente, el deepfake, que es parte de las funciones que ofrece la IA. Por lo que ofrece imágenes, sonidos y videos, con un alto grado de realismo. Entre sus técnicas, está la captura de movimiento el fase-swappping, combinando ambos aspectos (imagen y movimiento) para colocar los rostros de personas. Por lo que representa un riesgo, en este tipo de contexto, al percibirse como imágenes que dan una ilusión de autenticidad. De manera que, se configuran en material que representa un riesgo para la valoración judicial.

Por lo que son aspectos que requieren del dinamismo de la creación de protocolos claros de autentificación. Además, que la normativa debe contar con criterios precisos para evaluar las pruebas que son generadas por medio de la IA. En función de lo cual, deben imperar criterios uniformes, con reglas definidas que permita asegurar decisiones coherentes y proteger las garantías procesales ante la evolución de las TICs

Tabla 1. Principales técnicas de IA empleadas en la producción digital de material sexual infantil.

| Técnica / Herramienta | Descripción básica | Riesgo procesal principal |
|---|---|---|
| Modelos generativos (Stable Diffusion, Midjourney, DALL·E) | Crean imágenes a partir de descripciones textuales. | Dificultad para verificar el origen y la autenticidad del archivo. |
| Aplicaciones de "desnudo sintético" (nudify) | Eliminan digitalmente la ropa en fotografías reales mediante redes neuronales. | Confusión entre imagen original y manipulada; vulneración del derecho a la imagen. |
| Deepfakes | Superponen rostros o cuerpos mediante face-swapping y motion capture. | Riesgo de falsificación integral del contenido audiovisual. |
| Alteración parcial o montaje híbrido | Inserta fragmentos reales en escenas artificiales. | Mezcla de veracidad y falsedad que confunde la valoración judicial. |

Fuente: elaboración propia basada en diversas fuentes, tanto doctrinales como técnicas, acerca de la inteligencia artificial (IA) y la evidencia digital.

Por lo que se demuestra que son aspectos que afectan de manera directa a la administración de la justicia, más allá que una cuestión de adopción tecnológica. En función de lo cual deben contemplarse en el derecho penal criterios uniformes sobre la adecuada admisión de evidencias digitales.

Con lo cual, resulta prioritario avanzar hacia la creación de protocolos nacionales de preservación digital y autenticación de evidencia electrónica, acompañados de programas de capacitación continua para los operadores judiciales y peritos informáticos.

### *Aportes académicos*

La doctrina procesal penal ha desarrollado valiosos marcos conceptuales para comprender los desafíos que plantea la incorporación de la prueba digital generada mediante inteligencia artificial:

Tabla 2. Principales aportes doctrinarios sobre la valoración de la prueba digital.

| Autor / Año | Aporte principal | Perspectiva o implicación procesal |
|---|---|---|
| Binder (2000) | El modelo acusatorio moderno se basa en los principios de oralidad, contradicción e inmediación, que garantizan la transparencia y racionalidad del juicio penal. | Estos pilares deben preservarse aun frente a la virtualización o automatización del proceso, manteniendo la autenticidad del debate judicial. |
| Ferrajoli (2001) | La validez de una prueba no depende solo de su contenido, sino de la forma en que se obtiene y controla. | Las garantías procesales como la legalidad y la cadena de custodia son límites esenciales frente al poder punitivo del Estado. |
| Cafferata (2004) | Toda prueba debe someterse a control judicial efectivo, evitando que la técnica sustituya el juicio crítico del juez. | La verdad procesal no puede quedar librada a la automatización, sobre todo cuando el material probatorio electrónico puede ser manipulada. |
| Casey (2019) | Los principios generales del proceso penal son insuficientes frente a la complejidad del archivo digital. | Propone protocolos técnicos rigurosos, verificación de metadatos y controles criptográficos para garantizar autenticidad e inalterabilidad. |
| Muñoz Conde (2015) | La valoración probatoria debe respetar la presunción de inocencia y el principio de contradicción. | En pruebas derivadas de IA, la defensa debe poder realizar contrapericias y cuestionar los algoritmos utilizados. |
| Taruffo (2008) | La verdad procesal no puede depender únicamente de instrumentos técnicos o periciales. | Debe construirse mediante un diálogo racional entre las partes, con transparencia y control judicial. |
| Moya (2022) | Advierte sobre falsos positivos y errores judiciales cuando se admiten evidencias generadas por IA sin autenticación adecuada. | La expansión de los deepfakes obliga a reforzar la labor pericial y el control judicial previo a su admisión. |
| Redondo (2021) | La fiabilidad tecnológica no puede sustituir la racionalidad crítica del juez ni el principio de contradicción. | El problema radica tanto en la obtención como en la valoración de la prueba, que debe analizarse con independencia de toda fascinación tecnológica. |
| Couture (1947) y Maier (1996) | El proceso penal es, ante todo, una garantía de libertad frente al poder del Estado. | Las nuevas formas de prueba, incluidas las basadas en IA, solo son legítimas si respetan plenamente los derechos de defensa y el debido proceso. |
| Loreti (2020) | La sofisticación tecnológica de la prueba debe acompañarse de un fortalecimiento proporcional de las garantías procesales. | La eficiencia nunca puede justificar la flexibilización de los derechos fundamentales; la tecnología solo es válida bajo un modelo garantista. |

Fuente: elaboración propia con base en Binder (2000); Ferrajoli (2001); Cafferata Nores (2004); Casey (2019); Muñoz Conde (2015); Taruffo (2008); Moya (2022); Redondo (2021); Couture (1947); Maier (1996) y Loreti (2020).

## *Marco jurídico nacional y comparado sobre el uso y valoración de la prueba digital en el proceso penal*

### Marco normativo nacional

"El sistema jurídico ecuatoriano reconoce en la Constitución de 2008 el derecho al debido proceso, consagrado en el artículo 76, que garantiza a toda persona la posibilidad de defenderse, controvertir la prueba y exigir una motivación judicial adecuada" (Constitución de la Republica del Ecuador, 2008, art. 76). Estos principios constituyen el marco dentro del cual debe valorarse cualquier tipo de evidencia, incluida la digital. La Carta Magna establece, además, que ninguna prueba obtenida con violación de derechos fundamentales puede ser admitida, lo que supone un límite estricto frente a los riesgos de manipulación o falsificación propios de la inteligencia artificial.

"El Código Orgánico Integral Penal regula en su artículo 454 los principios de la prueba legalidad, pertinencia, contradicción y respeto al debido proceso, mientras que el artículo 456 establece que únicamente pueden valorarse aquellas pruebas obtenidas de manera lícita" (Código Orgánico Integral Penal, 2014, arts. 454 y 456). Aunque el COIP no menciona expresamente los contenidos digitales generados mediante inteligencia artificial, estos preceptos resultan aplicables por analogía, imponiendo al juez el deber de examinar si el material probatorio electrónico cumple con criterios de autenticidad e integridad antes de ser incorporada al proceso. Como opina Ferrajoli (2001), "la validez de la prueba depende no solo de su contenido, sino también de la forma en que es obtenida y controlada" (p. 623), lo que cobra especial relevancia en el tratamiento de material sintético.

El Código Orgánico General de Procesos (2015) y el Código Orgánico de la Función Judicial (2009), comprende el uso de medios electrónicos en la administración de justicia, en el que primen la digitalización de los procedimientos y una mayor eficiencia institucional. A pesar de ello, no existe uniformidad sobre la valoración de la prueba digital, por la propia complejidad que presenta. Esta falta de directrices concretas ha creado vacíos procesales que amenazan la legitimidad y la fiabilidad de la evidencia tecnológica presentada ante los tribunales".

Esta ausencia de regulación técnica traslada al juez la responsabilidad de decidir, caso por caso, sobre la admisibilidad y el valor probatorio de tales elementos, ampliando el margen de discrecionalidad judicial y, con ello, el riesgo de decisiones contradictorias y de inseguridad jurídica. De ahí la necesidad de establecer criterios uniformes que garanticen la integridad de la prueba digital y preserven la coherencia del sistema penal frente a los desafíos tecnológicos contemporáneos.

### Marco Normativo Internacional

En el ámbito internacional, la Convención sobre los Derechos del Niño (1989), ratificada por el Ecuador, obliga a los Estados a garantizar la protección integral de los menores frente a toda

forma de explotación sexual, incluso cuando esta ocurre en entornos digitales. Aunque el texto convencional no alude de manera expresa a la inteligencia artificial, una lectura evolutiva de sus principios permite inferir que la creación de material sexual infantil mediante tecnologías sintéticas vulnera la dignidad y el desarrollo integral de la niñez, valores fundamentales amparados por dicho instrumento.

De igual manera, el Convenio sobre Ciberdelincuencia de Budapest (2001),

> constituye el principal referente internacional en la materia. Este tratado fija estándares comunes para la preservación y autenticación de la evidencia electrónica, así como para la cooperación judicial entre los Estados frente a los delitos informáticos. Aunque Ecuador aún no lo ha ratificado, sus disposiciones técnicas ofrecen pautas útiles para el diseño de protocolos nacionales que fortalezcan la admisibilidad y la valoración de la prueba digital en el proceso penal.

La jurisprudencia internacional también ha desarrollado estándares interpretativos que buscan compatibilizar la innovación tecnológica con las garantías judiciales. En su Opinión Consultiva (2017),

> aunque referida originalmente a temas de identidad de género e igualdad, la Corte Interamericana de Derechos Humanos estableció un principio general aplicable por analogía: los sistemas de justicia deben adaptarse a las transformaciones sociales y tecnológicas sin debilitar el núcleo esencial del debido proceso ni los derechos fundamentales.

De manera concordante, el Tribunal Europeo de Derechos Humanos, en el caso Roman Zakharov vs. Rusia (2015), "precisó que la obtención y el uso de evidencia tecnológica deben someterse a mecanismos efectivos de control judicial y a criterios de proporcionalidad que aseguren la protección del derecho a un juicio justo."

Desde la doctrina, Luño (2004),

> afirma que los derechos fundamentales mantienen su vigencia aun frente a las transformaciones tecnológicas, y que el Estado de Derecho solo preserva su legitimidad cuando los procedimientos judiciales especialmente los de carácter penal aseguran de manera real y efectiva la protección de tales derechos.

Esta reflexión adquiere especial relevancia en el proceso penal actual, donde la incorporación de la prueba digital y la inteligencia artificial demanda una constante actualización técnica sin sacrificar las garantías esenciales del debido proceso.

### *Derecho comparado: experiencias internacionales*

Al observar cómo otros países abordan este tema, notamos que sus leyes y decisiones judiciales han establecido maneras de enfrentar los desafíos que presenta la evidencia digital generada por la IA.

Tabla 3. Respuestas normativas y jurisprudenciales frente a la prueba digital basada en inteligencia artificial.

| País | Normativa o caso relevante | Medida o criterio aplicado | Aporte principal |
|---|---|---|---|
| Alemania | Práctica judicial en casos tecnológicos complejos | Exigencia de doble pericia independiente en evidencias audiovisuales generadas o manipuladas con inteligencia artificial | Garantiza un contraste técnico objetivo antes de la admisión judicial y evita interpretaciones unilaterales. |
| España | (Ley Orgánica 1/2015) y (Tribunal Supremo, N.º 577/2019) | Establece sanciones por difusión de imágenes manipuladas y exige peritajes informáticos rigurosos. | Reafirma la cadena de custodia digital y consolida estándares probatorios técnicos y judiciales. |
| Estados Unidos | United States v. Thomas R. Nichols (2023) | Exige verificación criptográfica y validación experta independiente antes de admitir material digital como prueba. | Fija un precedente en la autenticación forense de archivos deepfake en procesos penales por explotación infantil. |
| Argentina | Ley N.º 27.590 ("Ley Micaela Ortega", 2020) | Fortalece fiscalías especializadas y establece protocolos de preservación de metadatos y cadena de custodia digital. | Mejora la trazabilidad y autenticidad de los archivos electrónicos, equilibrando eficacia investigativa y respeto al debido proceso. |

Fuente: elaboración propia a partir de legislación y jurisprudencia comparada (Ley Orgánica 1/2015; Tribunal Supremo, Sentencia N. º 577/2019; United States v. Nichols, 2023; Ley 27.590, Argentina).

En resumen, los modelos de Alemania, España, Estados Unidos y Argentina nos muestran que la regulación de las pruebas digitales no puede limitarse solo a los aspectos técnicos. Es esencial que se incluya con mecanismos de control judicial, transparencia en la pericia y la cooperación internacional. Por lo que la adopción de la tecnología no debe condicionar la deliberación nacional. De manera que la validez de la prueba digital dependerá de los estándares técnicos adecuados.

### *Desafíos procesales y garantistas en la admisión de pruebas generadas mediante inteligencia artificial*

La aparición de las pruebas digitales desarrolladas a partir de la IA, al sistema de penal ecuatoriano se configura dentro de un contexto complicado. En el que el desarrollo tecnología lleva a que pueda significar cuestionamientos con los principios del debido proceso. A diferencia de la tangibilidad de la prueba física, las digitales son replicables con mayor facilidad, y pueden ser alteradas sin dejar constancia palpable de ello. Es un aspecto, que plantea la redimensión de los criterios de apreciación de la prueba.

El alto grado de realismo de las imágenes producidas por la IA, ha dado lugar también a su mal uso. Con acciones que son consideradas como nuevas formas de criminalidad digital, que, en el caso de menores de edad, implica una connotación sexual sin que intervengan de manera directa. En función de lo cual, se plantean distintos cuestionamientos, sobre su valoración e implicaciones de los elementos constitutivos de delitos.

El COIP en la actualidad no aborda si estas pruebas son aceptables, su validez y relevancia. En la práctica los jueces y fiscales deben utilizar criterios generales, en relación con su admisibilidad, e integridad, lo que resulta insuficiente ante la complejidad que plantea la IA. Por lo que plantea cuestionamientos en la práctica judicial, como el principio de inocencia, derecho a la defensa e impugnación de pruebas, ante el uso de imágenes que pueden pasar como reales.

El sistema de justicia en Ecuador necesita establecer de inmediato reglas claras para la aceptación, seguimiento y control de las pruebas digitales en los juicios. Además, jueces, fiscales y peritos deben recibir formación especializada y continua. Solo así podremos utilizar la tecnología en los procesos penales sin comprometer las garantías legales ni la búsqueda de la verdad en los tribunales.

### *Riesgo de autenticidad*

El primer gran problema con las pruebas digitales hechas por inteligencia artificial es saber si son reales. Estas herramientas pueden hacer imágenes, audios o videos que parecen totalmente verdaderos, pero que en realidad son falsos. Con sistemas muy avanzados, se pueden crear escenas completas, incluso sexuales, sin que nada de eso haya pasado de verdad.

Esto es muy grave cuando se trata de material infantil. La inteligencia artificial puede hacer imágenes falsas que parecen reales a primera vista. Entonces, en un juicio, ¿cómo podemos estar seguros de que un archivo digital muestra algo que realmente pasó y no es solo una creación?

No es solo un asunto técnico, sino que afecta directamente a las pruebas legales. Si no tenemos formas seguras de verificar las cosas, la validez de la prueba, el proceso legal y la confianza en la justicia están en peligro. Por eso, es muy importante tener reglas claras para rastrear, guardar y certificar los archivos digitales antes de usarlos en un juicio. Así, podemos estar seguros de que las pruebas son reales y que el proceso legal es justo.

### *Riesgo de manipulación*

Otro problema tiene que ver con cómo se opera el archivo digital. La inteligencia artificial (IA) no solo hace que sea posible inventar o crear imágenes o videos, sino que también deja cambiar archivos reales de una forma que es muy difícil de notar. A veces, fotos verdaderas de niños, que se sacan de redes sociales, se pueden cambiar digitalmente para ponerlas en escenas sexuales, lo que daña mucho la privacidad y el honor de los niños.

La Internet Watch Foundation (2023), "afirma que este tipo de contenido falso representa una de las mayores amenazas en el mundo del ciberdelito sexual infantil, precisamente porque las alteraciones son prácticamente imperceptibles, aun para los peritos forenses."

Desde el punto de vista legal, la posibilidad de que se cambie algo pone en riesgo si la evidencia es legal, completa y creíble. Tal como respalda Beltrán (2007), "para que un juez decida bien, toda la evidencia tiene que poder ser verificada, revisada y discutida. Si un juzgador no entiende cómo se puede cambiar algo digitalmente, podría aceptar una prueba falsa y basar su decisión en algo que no es real, lo que dañaría la presunción de inocencia y la seguridad legal."

Por esto, el sistema penal de Ecuador necesita reglas expertas para saber si algo ha sido cambiado digitalmente, confirmar de dónde vienen los archivos y verificar que nada cambie desde que se obtienen hasta que se usan en el juicio. Si el país no hace esto, los juzgados podrían aceptar cosas falsas sin saberlo, lo que no solo pondría en riesgo que las decisiones sean justas, sino también la fe de la gente en el sistema penal.

### *Riesgo de contradicción*

El tercer problema importante tiene que ver con el principio de contradicción. Esta regla es súper importante porque deja que las partes cuestionen y discutan las pruebas que se presentan en su contra. Este principio es clave en los juicios orales y para el derecho a la defensa. Pero, si las pruebas vienen de sistemas raros o de programas de inteligencia artificial (IA) que nadie entiende bien (ni siquiera los que saben del tema), la defensa puede estar en desventaja. No tienen las herramientas ni a los expertos para pelear contra las pruebas de forma correcta. Esto crea una desigualdad en el juicio, lo cual va en contra del artículo 76 de la Constitución de Ecuador, que dice que todos deben tener las mismas oportunidades en un juicio penal.

Fenoll (2018), señala que "si no entendemos cómo funcionan los algoritmos, la tecnología puede volverse algo que nadie podrá controlar." El conocimiento técnico reemplazara la discusión lógica y los juicios orales se volverán menos transparente. Por eso, para poder contradecir pruebas digitales hechas con inteligencia artificial (IA), no basta con solo tener la oportunidad de refutar un informe pericial. Se necesita tener acceso a herramientas forenses, que los jueces, fiscales y defensores se capaciten constantemente, y que se entienda cómo se crearon, verificaron y ratificaron las pruebas.

Así es la única forma de que la contradicción no sea solo una formalidad vacía y que el juicio penal no pierda su equilibrio. Al final, asegurar que se pueda contradecir la prueba tecnológica no es algo extra que se pide, sino algo necesario para que el juicio sea justo y la gente confíe en la justicia penal.

### *Implicaciones procesales de la evidencia digital generada por inteligencia artificial (IA)*

Cuando usamos como prueba en un juicio archivos digitales creados por IA, se complican las cosas para el juez y los abogados. Lo más difícil es estar seguros de que esas pruebas sean reales, que no las alteraron y de dónde salieron. Como estas pruebas no son algo físico, es fácil modificarlas sin que se note, y eso hace que no podamos confiar mucho en ellas, poniendo en riesgo todo el juicio.

Pero no solo es que puedan cambiar las pruebas, sino que, además, los abogados defensores a veces no tienen ni idea de cómo revisar bien esos archivos creados por IA. Esto hace que no estén en igualdad de condiciones con la otra parte y que no puedan defender bien a su cliente, lo cual es muy importante en un juicio justo.

Así que, cuando un juez tiene que decidir si una prueba de este tipo es válida, necesita saber de leyes, pero también entender cómo funcionan las nuevas tecnologías, cómo verificar que un archivo es real y cómo guardarlo de forma segura. La ausencia de estas capacidades podría conducir a decisiones fundadas en evidencias cuya fiabilidad técnica no ha sido verificada con rigor.

En consecuente, las implicaciones procesales derivadas de la inteligencia artificial demandan una reconfiguración integral de las prácticas judiciales. Es necesario establecer programas permanentes de capacitación tecnológica para jueces, fiscales y defensores; crear protocolos uniformes sobre cadena de custodia digital; y exigir que cada procedimiento de verificación o análisis de archivos electrónicos quede debidamente documentado y disponible para control de las partes. Solo de esta manera podrá mantenerse el equilibrio entre el avance tecnológico y los principios que sostienen el proceso penal garantista.

### *Reflexión crítica sobre la regulación de la prueba digital en el proceso penal*

El examen del marco normativo nacional e internacional muestra que, si bien existe un consenso general respecto de los principios que deben regir la prueba digital ya sean la legalidad, autenticidad, contradicción y debido proceso, aún persiste un vacío regulatorio frente a los contenidos sintéticos producidos mediante inteligencia artificial. En el caso ecuatoriano, aunque la Constitución y las normas procesales ofrecen fundamentos aplicables por analogía, la falta de lineamientos técnicos uniformes genera criterios dispares que afectan la coherencia del sistema penal y la seguridad jurídica de los procesos.

En este contexto, la doctrina coincide en que el verdadero reto no radica en la existencia de la prueba digital, sino en establecer mecanismos que permitan su incorporación sin debilitar los pilares del debido proceso. Tal como señala Ferrajoli (1995), “la legitimidad del poder punitivo depende del respeto estricto a las garantías procesales, especialmente cuando se enfrenta a nuevos medios de prueba capaces de alterar la presunción de inocencia o el principio de contradicción”.

Los cambios que plantea el uso de la IA en distintos ámbitos sociales también deben ser acogidos dentro del jurídico, con el fin de que las TICs contribuya, garantizando derechos fundamentales en los procesos judiciales.

## Metodología

La investigación se desarrolló bajo un enfoque cualitativo y descriptivo con el objetivo de profundizar en la temática de estudio desde una perspectiva legal, doctrinal y jurisprudencial. Se dio prioridad al análisis normativo sobre la medición estadística, centrándose en los riesgos de carácter procesal y los aspectos técnico-legales fundamentales para garantizar la validez de las pruebas.

Para llevar a cabo la investigación, se aplicaron varios métodos. El método dogmático-jurídico se empleó para examinar el contenido normativo positivo, lo que permitió identificar tanto disposiciones explícitas como posibles lagunas. Gracias a este método, se fundamentó la descripción del actual marco legal y se pudo determinar su alineación con los tratados internacionales.

Paralelamente, se utilizó el método hermenéutico con el fin de reinterpretar normas desde un enfoque axiológico, que prioriza la protección de los derechos fundamentales. Este enfoque fue crucial para analizar elementos jurisdiccionales y reinterpretar la cadena de custodia digital, integrando los principios de proporcionalidad y minimización de datos. Finalmente, se aplicó el método analítico-sintético, a través del cual el problema fue considerado desde distintas aristas mediante un análisis detallado de sus componentes, para luego ser sintetizados en un marco propositivo de directrices procesales.

La población estuvo constituida por un conjunto de relevantes fuentes jurídicas, incluyendo normas nacionales (como la Constitución de la República del Ecuador - CRE y el Código Orgánico Integral Penal - COIP), tratados internacionales (como la Convención Americana sobre Derechos Humanos - CADH y el Convenio de Budapest), así como doctrina vinculante y jurisprudencia pertinente.

La muestra fue seleccionada de manera no probabilística e intencional con el propósito de maximizar su relevancia y representatividad crítica. Esta incluyó textos normativos, artículos científicos y casos judiciales. Se recurrió al derecho comparado tomando en cuenta a España, por su significativo nivel de regulación en el marco de la Unión Europea sobre pruebas digitales; a Argentina, por sus similitudes procesales penales con Ecuador; y a Estados Unidos (EEUU), por contar con una jurisprudencia pionera en la autentificación de evidencia digital. De esta manera, se contrastaron sistemas ya establecidos (España y EEUU) con sistemas emergentes (Argentina y Ecuador).

La técnica de investigación principal comprendió una revisión de fuentes secundarias, seguida del registro, clasificación y análisis de los datos obtenidos. Esta técnica se complementó con un análisis comparativo de la jurisprudencia seleccionada. Es importante señalar que la investi-

gación se enfrentó a ciertas limitaciones, como la ausencia de datos primarios, lo cual restringió la validación empírica práctica de las conclusiones. Además, el enfoque intencional de la muestra pudo haber introducido un sesgo. Por último, existió una dependencia a las fuentes accesibles, sin contar con acceso a expedientes judiciales confidenciales para un análisis más profundo.

## Desarrollo

Los resultados destacan que el marco legal ecuatoriano, en especial la CRE y COIP, reconocen los principios fundamentales, como la presunción, la validez, cadena de custodia y la necesidad de fundamentar las decisiones judiciales. Pero que, por otra parte, no se contemplan parámetros técnicos referente a la admisión, autentificación o evaluación de pruebas generadas por IA, lo que da lugar a vacíos legales y criterios inconsistentes dentro de lo que es la práctica judicial.

En este contexto, autores como Casey, Ferrajoli, y Tarruffo resaltan diferencias conceptuales en el tratamiento de la prueba digital. Ferrajoli, desde su teoría del garantismo penal, enfatiza la prueba como garantía de los derechos fundamentales y la verdad procesal, en el que se priorice su rol en la aplicación axiomática de normas, con la finalidad de evitar arbitrariedades, en un enfoque epistemológico que vincula la prueba a la correspondencia con la realidad ontológica. Tarrufo, adopta una perspectiva racionalista en la prueba de los hechos, centrada en la incertidumbre y la probabilidad, por lo que propone métodos para aproximar la verdad judicial por medio de narrativas probatorias coherentes, distingue la realidad procesal, de la verdad absoluta, incorporando elementos persuasivos y culturales en la valoración.

Por su parte, Casey se enfoca en la cadena de custodia técnica, la autenticidad forense, por lo que atiende a un marco práctico y empírico para admisibilidad en tribunales, priorizando herramientas como los metadatos o el hashing, sobre consideraciones netamente garantitas.

Se identificaron tres aspectos clave en el que se concentran lo mayores riesgos procesales. El primero de ellos es el relacionado con la autenticidad, en el que se percibió que las herramientas de generación sintética crean imágenes, videos, y sonidos que parecen reales. La simulación de la realidad implica a que se cuestione la autenticidad de la evidencia.

El segundo se refiere a la manipulación, la IA implica esa capacidad, al generar imágenes o videos con un alto nivel de detalle, que resulta difícil de detectarlo a simple vista. Lo que repercute en aspectos, como la preservación de su integridad de prueba y el peligro de la cadena de custodia. Lo que plantean que se establezca mayores controles y peritajes pertinentes en el área, para una identificación más precisa.

Finalmente, en la contradicción, se muestra una desigualdad técnica entre las partes en el proceso. Porque es necesario contar con formación y recursos para identificar pruebas digitales complejas. Tal situación implica un desbalance en el proceso, limitando el derecho a la defensa. Con lo cual, es preciso la creación de unidades periciales especializadas en el análisis de la IA y los delitos informáticos.

Desde el análisis penal sustantivo, son riesgos que se agravan en los casos de pornografía infantil generada por IA sin víctima física directa, en el que la teoría del bien jurídico protegido justifico la intervención penal, por medio de la lesividad simbólica: conforme con la doctrina de Ferrajoli, la mera representación virtual perpetua una violencia simbólica, que menoscaba la dignidad la dignidad infantil y normaliza conductas predatorias, por lo que se extiende el ius punendi, más allá de daños materiales para salvaguardar bienes universales como la integridad moral colectiva, alineándose con el derecho penal de riesgo que penaliza peligros abstractos sin que se requiera de lesividad concreta, pero en el que se respeta principios de mínima intervención para así evitar expansiones injustificadas.

Por su parte, el análisis comparativo revela que otros países han desarrollado criterios definidos. En Alemania existe una doble evaluación independiente, como paso previo para aceptar pruebas digitales de alta complejidad. En España, la evidencia digital no puede considerarse como válida sin un adecuado peritaje informático, en el que se confirme la integridad de los datos y recorrido técnico.

En Argentina, la Ley Micaela Ortega introdujo normas técnicas para la preservación digital de la evidencia, fortaleció las fiscalías especializadas. En EEUU, en su jurisprudencia discute la autenticidad de un video que se genera por deepfake, a los que debe aplicarse peritajes y certificación criptográfica.

Son elementos, que fundamentan la necesidad de encontrar un equilibrio entre la precisión técnica y la protección de las garantías procesales. Se han establecido mecanismos que combinan el control, seguimiento y respeto del debido proceso. En función de lo cual, Ecuador debe establecer protocolos para la verificación digital y exigencias de peritajes independientes, antes de su aceptación de pruebas tecnológicas en juicio.

## Discusión

La generación de pornografía infantil por medio de la IA, es uno de los desafíos más importante para la actualidad del derecho procesal penal. Es un fenómeno que no solo comprende nuevas formas de delito, lo que amerita que se replanten las formas en cómo se obtiene, autentica y valoran las pruebas digitales en el ámbito judicial. El estudio demuestra que el marco legal incluye principios fundamentales como la legalidad de la prueba, la preservación de la cadena de custodia y la motivación judicial. No obstante, se carece de mecanismos normativos y técnicos para la verificación de la autenticidad de los archivos generados por la IA. Es un vacío que resulta en inseguridad jurídica, al dejarse en la discrecionalidad del juez la admisión o no de las evidencias tecnológicas.

Desde las experiencias internacionales, muestran cómo se han desarrollados aspectos o elementos clave, como el caso alemán, en el que se exige la doble pericia independiente en casos

complejos; en España, en el que la validez de la material probatorio electrónico se condiciona a la integridad de los datos, por examen informático previo; la creación de fiscalías especializadas, como el caso de Argentina; y el caso de los EEUU, en el que se destaca la necesidad de verificaciones criptográficas y peritajes especializados.

Son experiencias que muestran la evolución del derecho ante los aspectos vinculados con las TICs, las cuales pueden ser integradas al proceso penal, sin que signifique comprometer garantías procesales. Por lo que Ecuador, debe establecer políticas públicas de justicia digital que establezca protocolos de judiciales para la autentificación, trazabilidad y conservación de evidencias digitales.

Las cuestiones vinculadas a la IA, en la administración de justicia, comprende un aspecto ético y estructural, que refine las conceptualizaciones sobre la verdad procesal y redimensiona la relación entre juez, prueba y realidad. De manera, que es necesario emplear la racionalidad humana en los aspectos que involucre desafíos de distinguir la realidad con la virtualidad compleja de la IA. En este contexto, resulta imperativo que se combine la actualización legislativa con la capacitación técnica de los operadores de justicia, que se dota de herramientas especializadas, que permiten comprender los alcances de la IA y realizar una valoración crítica rigurosa, que se alinean con las exigencias del debido proceso penal.

Los resultados destacan que el CRE y el COIP, reconocen principios fundamentales en el proceso penal. No obstante, no contemplan parámetros técnicos para la admisión, autentificación de pruebas generadas por el IA, lo que genera vacíos legales y criterios inconsistentes en las prácticas judiciales.

Los elementos identificados en el análisis comparativo, destaca la necesidad de equilibrar precisión técnica y garantías procesales, proponiendo que Ecuador establezca protocolos de verificación digital y peritajes independientes obligatorios antes de admitir pruebas tecnológicas en juicio. Este equilibrio exige configurar una política que combine actualización legislativa con capacitación técnica continua de los operadores judiciales, habilitándolos para el manejo de herramientas como análisis de datos, e identificadores de anti-fake, en el que se asegure una valoración crítica que preserve la verdad procesal y el debido proceso.

Se debe configurar en la realidad actual, una política que combine la actualización de la legislación con la capacitación de la tecnología de los operadores de justicia. El manejo por parte de los operadores de justicia de herramientas técnicas para comprender los alcances de la IA, empleando una adecuada valoración critica que exige el proceso penal. En este contexto, es fundamental una política integral que combine la actualización legislativa con la capacitación técnica de los operadores de justicia, que los dota de herramientas especializadas que les permite comprender los alcances del IA y realizar una valoración crítica rigorosa, que se vinculen con la exigencia del derecho procesal penal.

### *Derechos penalmente protegidos vulnerados por la pornografía infantil generada mediante inteligencia artificial*

Los aspectos relacionados a las implicaciones procesales y los retos en la presentación de pruebas, es necesario enfocarse en aquellos derechos que se encuentran protegidos penalmente. La generación de pornografía infantil, por medio de la IA, es un reto para los derechos que debe proteger el derecho y para su persecución penal. Aunque se trate de un contenido que no involucra menores de edad reales, si afectan la dignidad humana, la integridad moral, como principios constitucionales en la CRE y en los diferentes tratados internacionales en DDHH.

En el ámbito penal, se afecta la indemnidad sexual. Como señala Ferrajoli (2001),

> el Derecho Penal tiene un papel fundamental al actuar como una garantía frente a las formas de poder que menoscaban la dignidad humana; por lo tanto, no sancionar estas conductas sería permitir una nueva forma de violencia simbólica contra la infancia. (p. 145)

Los riesgos de explotación que surgen al permitir la creación ilimitada de material que parece real son alarmantes, ya que generan un mercado de consumo que sigue perpetuando la victimización simbólica de los menores. Aunque no haya víctimas físicas, la existencia de estas representaciones digitales normaliza la erotización de la infancia y reproduce patrones culturales de abuso.

En el ámbito interno, el COIP (2014), establece sanciones para la producción y difusión de material sexual infantil en su artículo 103. Sin embargo, aún no aborda de manera clara las representaciones generadas por inteligencia artificial. Es un vacío que crea una zona de impunidad que va en contra de los principios de protección integral de la niñez. Con lo cual, se requieren reformas para abarcar las implicaciones del uso de las TICs. De manera que, se trata de prácticas que causan daño, así se traten de imágenes virtuales, en función de su impacto en la dignidad y la sociedad en su conjunto.

## Conclusión

### *Hallazgos:*

El sistema de justicia penal en Ecuador aún no tiene los parámetros jurídicos adecuados, para abordar las cuestiones de las pruebas digitales generadas por IA, en especial en lo relativo a la pornografía infantil. Es un vacío en la norma, que expone los aspectos relacionados a la falta de actualización de las leyes, y de la comprensión técnica de estas nuevas formas de evidencia digital.

Los principios inherentes el proceso penal mantienen su relevancia, pero requieren redimensión antes avances tecnológicas, replanteando el control judicial, la función pericial y la justicia efectiva sin comprometer derechos fundamentales.

La ausencia de protocolos sobre la autentificación y la trazabilidad digital crea incertidumbre en la valoración de las pruebas. La no existencia de criterios uniformes, los jueces se enfrentan a decisiones inconsistentes, que ponen en peligro la legitimidad del proceso. La experiencia en otros países muestra que es posible que se superen estas limitaciones, si se implementan mecanismos técnicos y periciales robustos, en conjunto con una necesaria cultura jurídica que atienda al impacto de las TICs.

El análisis comparativo demuestra que países como Alemania, España, Argentina y EEUU, han separado limitaciones similares por medio de mecanismos técnicos robustos, peritajes especializados, y una cultura jurídica adaptada al impacto de las TICs.

***Riesgos:***

Autenticidad comprometida, la capacidad de la IA para la generación de contenido sintético hiperrealista, cuestiona la veracidad de la evidencia, sin contar herramientas normativas o técnicas para su verificación.

Manipulación indetectable, la dificultad para identificar alteraciones a simple vista pone en peligro la integridad de la prueba y la cadena de custodia, exigiendo controles periciales avanzados.

Desigualdad procesal, la brecha técnica entre las partes limita el derecho a la defensa, al requerir formación y recursos especializados que no se encuentran disponibles uniformemente.

Inseguridad jurídica, la discrecionalidad judicial en la admisión de pruebas digitales complejas generan criterios inconsistentes, vulnerando la predictibilidad del proceso.

***Propuesta:***

Reformar el COIP para la inclusión de capítulo específico sobre archivo digital compleja, haciendo uso de terminología pertinente, y criterios de admisibilidad que se relacionen con estándares internacionales.

Protocolos nacionales que garanticen la autentificación y seguimiento de los archivos electrónicos. Son protocolos que debe contar con pasos claros y verificables, desde la obtención del archivo hasta su presentación en juicio, que asegura que su integridad pueda comprobarse.

Es necesario, que sean desarrolladas unidades judiciales especializadas en el análisis de material probatorio electrónico e IA, que puede ofrecer apoyo técnico a los tribunales en casos complejos.

Se debe fortalecer la capacitación continua de jueces, fiscales, defensores y peritos, no solo en relación a los aspectos tecnológicos, sino también a lo que es la protección de los derechos fundamentales y ética digital.

Es necesario contar con cooperación internacional en el ámbito de ciberdelincuencia es fundamental, con base al Convenio de Budapest, la jurisprudencia comparada.

El desarrollo de criterios de una ética judicial digital que guie el uso de tecnologías en el ámbito penal, bajo los principios de humanidad, proporcionalidad y dignidad. Es necesario atender al compromiso ético con la verdad, y de la defensa de los derechos fundamentales, remarcando los aspectos referentes a la realidad de la prueba, y de los elementos que le son parte.

## Referencias


Argentina. (2020). *Ley N.º 27.590 — Programa Nacional de Ciberseguridad "Ley Micaela Ortega"*. Boletín Oficial de la República Argentina, 23 de diciembre de 2020.

Asamblea General de las Naciones Unidas. (1989). *Convención sobre los Derechos del Niño*.

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180.

Binder, A. (2000). *Introducción al derecho procesal penal*. Ad-Hoc.

Cafferata Nores, J. L. (2004). *El proceso penal acusatorio*. Rubinzal-Culzoni Editores.

Casey, E. (2019). *Digital evidence and computer crime: Forensic science, computers and the Internet*. Academic Press.

*Código Orgánico de la Función Judicial* [COFJ]. (2009). *Registro Oficial Suplemento 544.*

*Código Orgánico General de Procesos* [COGEP]. (2015). *Registro Oficial Suplemento 506.*

Corte Interamericana de Derechos Humanos. (2017). *Opinión Consultiva OC-24/17: Identidad de género, e igualdad y no discriminación a parejas del mismo sexo**

Couture, E. J. (1947). *Fundamentos del derecho procesal civil*. Editorial B de F.

Ferrajoli, L. (1995). *Derecho y razón. Teoría del garantismo penal*. Trotta.

Ferrajoli, L. (2001). *Principia Iuris. Teoría del derecho y de la democracia*. Trotta.

Ferrer, J. (2007). *La valoración racional de la prueba*. Marcial Pons.

International Watch Foundation. (2023). *Annual report 2023: The state of online child sexual abuse material*. IWF.

Loreti, D. (2020). *Derecho, comunicación y nuevas tecnologías*. Siglo XXI Editores.

Lynch, C. (2000). *Autenticidad e integridad en el entorno digital: Una exploración*. Council on Library and Information Resources.

Maier, J. (1996). *Derecho procesal penal. Tomo I: Fundamentos*. Editores del Puerto.

Moya, L. (2022). Evidencia digital y garantías procesales en la era de la inteligencia artificial. *Revista Chilena de Derecho Penal y Criminología*.

Muñoz Conde, F. (2015). *Derecho penal: Parte general*. Tirant lo Blanch.

Nieva Fenoll, J. (2018). *Inteligencia artificial y proceso judicial*. Marcial Pons.

Pérez Luño, A. (2004). *Derechos humanos, Estado de derecho y Constitución*. Tecnos.

Redondo, G. (2021). Prueba sintética y debido proceso en el derecho penal contemporáneo. *Revista Iberoamericana de Derecho Procesal*.

Russell, S., & Norvig, P. (2012). *Inteligencia artificial: Un enfoque moderno*. Pearson Educación.

Taruffo, M. (2008). *La prueba de los hechos*. Marcial Pons.

Tribunal Europeo de Derechos Humanos. (2015). *Caso Roman Zakharov vs. Rusia*.

Tribunal Supremo (España). (2019). *Sentencia N.º 577/2019, de 26 de noviembre de 2019 (Recurso 3347/2018).* Sala de lo Penal del Tribunal Supremo.

## Autores

**Mateo David Arias Ordóñez.** Es un destacado profesional del Derecho con una sólida formación académica. Es titulado en esta disciplina, sobresaliendo por sus investigaciones pioneras en el sistema de justicia penal y el sistema constitucional del Ecuador. Su pasión por el aprendizaje y su compromiso con la excelencia académica lo han convertido en una figura respetada en el campo del Derecho.

**Andrea Lisseth Durán Ramírez.** Es una destacada profesora de Derecho Penal y Constitucional con una sólida formación académica. Posee una maestría en la especialidad, sobresaliendo por sus investigaciones pioneras en el sistema de justicia penal y el sistema constitucional del Ecuador. Su pasión por la docencia y su compromiso con la excelencia académica la han convertido en una figura respetada en el campo del Derecho Penal y Constitucional.

## Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Agradecimiento

Universidad Católica de Cuenca.

Nota

El artículo es original y no ha sido publicado previamente.