LEX, Revista de Investigación en Ciencias Jurídicas
Volumen 9, N° 34 / julio-septiembre 2026
ISSN-e: 2631-2735 / pp. 1-18
https://doi.org/10.33996/revistalex.v9i34.553
Artículo de investigación

LEX
Revista de Investigación en Ciencias Jurídicas
https://revistalex.org

Vacíos normativos en delitos con inteligencia artificial en Ecuador

Normative gaps in AI-related crimes in Ecuador.

Linda Azucena Anchundia Castro
la.defensalegal.ec@gmail.com
Domenica Alejandra Guevara López
domenicaguevara28@gmail.com
Edward Fabricio Freire Gaibor
edwfreireg@gmail.com
Jorge Luis Gonzabay Flores
j.l.gonzab@hotmail.com

Universidad Técnica de Machala. Machala, Ecuador

https://doi.org/10.33996/revistalex.v9i34.553

Palabras clave:
Deepfake; Derecho penal; Inteligencia artificial; Phishing; Prueba digital

Keywords:
Deepfake; Criminal law; Artificial intelligence; Phishing; Digital evidence

Historia del artículo:
Artículo recibido: 05 de junio 2026 /
Aceptado: 31 de julio 2026 /
Publicado: 27 de agosto 2026

Cómo citar:
Anchundia Castro, L. A., Guevara López, D. A., Freire Gaibor, E. F., & Gonzabay Flores, J. L. (2026). Vacíos normativos en delitos con inteligencia artificial en Ecuador. *Revista Lex 9*(34). 1-18. https://doi.org/10.33996/revistalex.v9i34.553

Resumen

El avance acelerado de la inteligencia artificial ha generado nuevas modalidades de criminalidad digital, como los deepfakes y el phishing automatizado, cuya complejidad supera la capacidad de respuesta del ordenamiento jurídico ecuatoriano. El objetivo del presente estudio fue analizar los vacíos normativos y procesales existentes en la persecución penal de estos delitos en Ecuador. La investigación se desarrolló bajo un enfoque cualitativo, mediante análisis doctrinal, normativo y comparado. Los resultados evidencian deficiencias en la tipificación penal, dificultades probatorias y limitaciones en la obtención de evidencia digital. Se concluye que el marco jurídico vigente resulta insuficiente, siendo necesario incorporar reformas legales y protocolos especializados que permitan una adecuada persecución penal de delitos cometidos mediante inteligencia artificial.

Abstract

The rapid advancement of artificial intelligence has given rise to new modalities of digital criminality, such as deepfakes and automated phishing, whose complexity exceeds the responsive capacity of the Ecuadorian legal system. The objective of this study was to analyze the existing normative and procedural gaps in the criminal prosecution of these offenses in Ecuador. The research was conducted under a qualitative approach, utilizing

doctrinal, normative, and comparative analysis. The results reveal deficiencies in criminal characterization, evidentiary challenges, and limitations in obtaining digital evidence. It is concluded that the current legal framework is insufficient, necessitating the incorporation of legal reforms and specialized protocols to enable the effective criminal prosecution of offenses committed through artificial intelligence.

Introducción

La inteligencia artificial ha transformado de manera profunda los mecanismos de manipulación digital y, en consecuencia, ha puesto en riesgo la seguridad jurídica, la privacidad, la honra y la imagen de las personas. Entre estas nuevas formas de alteración tecnológica, los deepfakes ocupan un lugar central, puesto que consisten en contenidos de audio, imagen o video que algoritmos de aprendizaje profundo crearon o manipularon para simular con notable realismo la identidad de una persona. Dicha tecnología puede tener un uso legítimo en el ámbito educativo o científico; sin embargo, también puede servir para finalidades ilícitas, como la difusión de información falsa, la suplantación de identidades o la fabricación de evidencias audiovisuales falsas dentro de un conflicto jurídico (Chesney y Citron, 2019).

En el ámbito del Derecho Penal, los deepfakes constituyen una problemática de gran envergadura, ya que dificultan la identificación del autor material, la verificación de la autenticidad del material digital y la valoración probatoria en el marco de un proceso judicial. Además, su elevado grado de realismo puede generar confusión entre las víctimas, la ciudadanía y los cuerpos encargados de la investigación. Por esa razón, el uso abusivo de esta tecnología no debe ser estudiado únicamente como un problema técnico, sino también como un problema jurídico que exige una respuesta categórica por parte del ordenamiento penal ecuatoriano (Miró Llinares, 2018). En esta misma línea, la doctrina reciente ha señalado que los deepfakes representan una amenaza epistémica para la sociedad, en tanto erosionan la capacidad de los individuos para distinguir entre contenidos auténticos y fabricados, lo cual debilita la confianza en la información audiovisual (Fallis, 2021).

En Ecuador, el Código Orgánico Integral Penal regula algunos delitos informáticos; no obstante, no contempla de manera específica las conductas relativas a la creación, difusión o uso malintencionado de deepfakes. Esa omisión normativa puede generar vacíos legales a la hora de investigar, procesar y sancionar este tipo de conductas. En consecuencia, pueden existir situaciones en las que cierta acción realizada mediante deepfakes no encaje adecuadamente en las diversas tipologías penales vigentes, lo que

podría afectar la protección de los derechos fundamentales y la eficacia del sistema penal (Asamblea Nacional del Ecuador, 2014).

La rápida evolución de la inteligencia artificial ha incrementado la complejidad de la criminalidad digital a escala global. Organismos internacionales como la UNODC han advertido que los delitos cibernéticos, incluidos aquellos que involucran contenidos sintéticos, representan un desafío creciente para los sistemas de justicia penal, debido a la dificultad para atribuir responsabilidad, preservar la cadena de custodia y verificar la autenticidad de la evidencia digital (United Nations Office on Drugs and Crime [UNODC], 2021).

De igual forma, la UNESCO ha subrayado la necesidad de que los Estados desarrollen marcos éticos y jurídicos que regulen el uso de la inteligencia artificial y protejan los derechos fundamentales frente a posibles abusos tecnológicos (UNESCO, 2021). Asimismo, estudios empíricos recientes han demostrado que los contenidos sintéticos de carácter político pueden alterar la percepción de la realidad y debilitar la confianza pública en las instituciones democráticas, lo cual evidencia la urgencia de respuestas regulatorias integrales (Vaccari y Chadwick, 2020).

En el ámbito del derecho comparado, la Unión Europea aprobó el Reglamento (UE) 2024/1689, conocido como Ley de Inteligencia Artificial, que establece obligaciones de transparencia para los contenidos generados o manipulados mediante inteligencia artificial, incluidos los deepfakes. Dicha norma exige que los proveedores de sistemas de IA informen a los usuarios cuando el contenido haya sido generado o alterado artificialmente, en particular cuando pueda inducir a error sobre su autenticidad (Parlamento Europeo y Consejo de la Unión Europea, 2024). Este marco regulatorio demuestra que otros ordenamientos jurídicos ya han reconocido la necesidad de abordar de forma específica los riesgos derivados de los contenidos sintéticos.

En América Latina, Chile promulgó la Ley 21.459 en 2022, que modernizó la legislación sobre delitos informáticos y la adecuó al Convenio de Budapest. Si bien dicha norma no contempla expresamente los deepfakes, sirve como referente regional para la actualización de los tipos penales frente a las nuevas formas de criminalidad digital (Biblioteca del Congreso Nacional de Chile, 2022). En contraste, Ecuador mantiene una regulación penal más general y fragmentada, lo que evidencia la urgencia de revisar el Código Orgánico Integral Penal para ofrecer respuestas más precisas ante las conductas realizadas mediante inteligencia artificial.

La razón de ser de este estudio radica en la necesidad de analizar cómo el ordenamiento jurídico ecuatoriano responde a la utilización delictiva de los deepfakes. Lo anterior importa porque la utilización de esta tecnología podría poner en peligro bienes jurídicos como la intimidad, la imagen, la honra, la identidad y la fe pública en el contenido digital. Además, existe la preocupación de que esta situación aumente en los próximos años, toda vez que la facilidad en el acceso a herramientas de inteligencia artificial tiende a

ser cada vez mayor. Por lo tanto, resulta imprescindible estudiar si la norma penal ecuatoriana es suficiente o si es necesario modificarla para responder a dicha forma de delincuencia digital.

Ante este panorama, la presente investigación formula la siguiente pregunta: ¿Cuáles son los vacíos normativos y procesales que enfrenta el ordenamiento jurídico penal ecuatoriano en la persecución de delitos cometidos mediante inteligencia artificial, en particular aquellos relacionados con el uso de deepfakes? El objetivo general consiste en analizar dichos vacíos normativos y procesales. Los objetivos específicos son: identificar las conductas delictivas que pueden realizarse mediante deepfakes; examinar las limitaciones del Código Orgánico Integral Penal ante esta modalidad de delincuencia digital; analizar las dificultades probatorias que surgen en la investigación de contenidos audiovisuales manipulados; y proponer criterios jurídicos que contribuyan a la regulación y persecución penal de los deepfakes en el contexto ecuatoriano.

Método

La presente investigación adoptó un enfoque cualitativo, enmarcado en el paradigma interpretativo, porque su finalidad consistió en analizar e interpretar los vacíos normativos y procesales del ordenamiento jurídico ecuatoriano respecto de los delitos que involucran inteligencia artificial, en particular aquellos vinculados al uso de deepfakes. Dicho enfoque permitió al equipo investigador examinar de manera crítica la normativa vigente, la doctrina especializada, la jurisprudencia disponible y el derecho comparado.

La investigación tuvo un carácter descriptivo con alcance analítico, ya que permitió identificar las principales características jurídicas de los delitos que involucran inteligencia artificial, describir las limitaciones de la legislación ecuatoriana y analizar críticamente sus implicaciones en la persecución penal y en la protección de los derechos fundamentales. El diseño de investigación fue documental-jurídico y se sustentó en la revisión de fuentes secundarias especializadas. El equipo investigador analizó normas jurídicas nacionales e internacionales, doctrina científica, artículos de revistas académicas indexadas, instrumentos internacionales, documentos institucionales, proyectos normativos y bibliografía especializada sobre inteligencia artificial, prueba digital y derecho penal.

Para la revisión documental, el equipo consultó bases de datos indexadas como Scopus, Dialnet y Redalyc, así como repositorios legislativos oficiales. Las ecuaciones de búsqueda incluyeron combinaciones como ('inteligencia artificial' AND 'derecho penal') OR ('deepfakes' AND 'delito') OR ('prueba digital' AND 'proceso penal'). El periodo temporal abarcó desde 2018 hasta 2024. Los criterios de inclusión exigieron documentos con respaldo académico, legislación vigente y jurisprudencia accesible. Por

el contrario, el equipo excluyó artículos de mera opinión, publicaciones de divulgación y documentos sin sustento científico.

La selección de las fuentes documentales respondió a criterios de pertinencia, actualidad y relevancia temática. El equipo priorizó publicaciones científicas, legislación vigente y documentos de organismos nacionales e internacionales vinculados con la regulación de la inteligencia artificial y los delitos informáticos. Asimismo, descartó documentos de carácter meramente divulgativo o sin respaldo académico.

La investigación empleó tres métodos complementarios. El método analítico permitió examinar los elementos jurídicos que integran la problemática objeto de estudio. El método comparativo posibilitó el contraste entre la regulación ecuatoriana y las experiencias normativas de otros ordenamientos jurídicos, en especial la Unión Europea, Chile y legislaciones de interés. El método jurídico facilitó el estudio y la interpretación de las normas constitucionales, penales y procesales que intervienen en el desarrollo de la investigación.

El equipo investigador aplicó como técnicas la revisión documental, el análisis normativo, el análisis doctrinal y el análisis jurisprudencial. Estas técnicas permitieron identificar los vacíos regulatorios, examinar la suficiencia del derecho positivo nacional y evaluar las circunstancias que dificultan la prueba en casos de utilización de inteligencia artificial para la ejecución de delitos. Los instrumentos de investigación consistieron en fichas bibliográficas, fichas normativas y matrices de análisis comparativo. A través de estos instrumentos, el equipo organizó la información recopilada y facilitó los procesos de clasificación, sistematización e interpretación del derecho.

El procedimiento metodológico siguió las siguientes etapas: primero, el equipo identificó y recopiló las fuentes documentales; segundo, revisó la normativa nacional e internacional; tercero, analizó la doctrina y la jurisprudencia en materia de inteligencia artificial y deepfakes; cuarto, comparó la regulación ecuatoriana con las experiencias de otros ordenamientos jurídicos; quinto, sistematizó la información obtenida; y sexto, analizó e interpretó los hallazgos a la luz del marco jurídico vigente.

Finalmente, el equipo investigador analizó la información mediante la técnica del análisis de contenido jurídico y la organizó en categorías temáticas predefinidas: vacíos normativos, tipificación penal, prueba digital, responsabilidad penal, protección de derechos fundamentales y propuestas de actualización normativa. Esta organización garantizó la coherencia entre los objetivos de investigación, el desarrollo del estudio y las conclusiones.

Resultados

Los resultados de la investigación se ordenaron a partir del análisis normativo, doctrinal y jurisprudencial del uso delictivo de la inteligencia artificial. Dicha tecnología se manifiesta, sobre todo, a través de los deepfakes y otras manipulaciones digitales de la identidad de las personas. Este proceso de estudio permitió al equipo investigador concluir que el ordenamiento jurídico ecuatoriano cuenta con normas generales aplicables a determinados delitos informáticos, a la intimidad, la honra, la imagen y la suplantación de la identidad. Sin embargo, esas disposiciones no establecen de un modo expreso las formas de creación, difusión y uso malicioso de los contenidos que la inteligencia artificial genera.

De lo expuesto se desprende un problema jurídico significativo: las nuevas formas de criminalidad digital no se ajustan de manera completa a los tipos penales tradicionales. Por consiguiente, la persecución penal de estas conductas puede enfrentar limitaciones de tipificación, dificultades probatorias, carencia de criterios técnicos uniformes y ausencia de una regulación que reconozca expresamente a la inteligencia artificial como medio de comisión. Los hallazgos se distribuyen en las categorías obtenidas durante el análisis de contenido jurídico. En cada categoría se distingue entre la información proveniente de las fuentes del análisis respectivo y los resultados que otorga el contraste de las fuentes con el ordenamiento jurídico ecuatoriano.

La inteligencia artificial como medio comisivo de nuevos delitos digitales

La inteligencia artificial ha pasado de ser únicamente una herramienta tecnológica de acompañamiento a constituir un posible medio comisivo de conductas delictivas. El análisis documental pone de manifiesto que estas herramientas pueden generar textos, imágenes, audios, vídeos y perfiles digitales falsos, además de simular la identidad de una persona con un grado de realismo difícil de detectar a partir de la observación común y corriente. Esto cobra una importante trascendencia ante la posibilidad de utilizar la tecnología para afectar la honra, la intimidad, la imagen, la seguridad de las personas, la reputación, la libertad sexual, la confianza pública y la estabilidad de los procesos judiciales o electorales.

El uso de la inteligencia artificial en los deepfakes supone que resulta posible crear contenidos audiovisuales en los que parece que una persona hace o dice algo que nunca ha hecho ni dicho. Este efecto puede generar un riesgo mayor al que puede producirse con otras modalidades de falsificación tradicional, dado que el contenido audiovisual y sonoro suele llevar aparejado un mayor efecto psicológico y social. La víctima no solamente puede experimentar un perjuicio personal, sino también la pérdida de prestigio ante su familia, su círculo laboral, académico o público. Además, cuando el contenido ingresa en las redes informáticas, su difusión es rápida y su eliminación es, en ocasiones, muy difícil.

Con base en la valoración hecha, el equipo investigador arribó a la conclusión de que la inteligencia artificial no constituye per se una conducta delictiva, pero sí puede operar

como un medio que agrava la posibilidad de fraude, la rapidez de su difusión y la gran magnitud del perjuicio. Su relevancia penal vendrá determinada por la finalidad con la que se utiliza, el bien jurídico afectado y la consecuencia producida.

Desde este prisma, la inteligencia artificial modifica la manera de cometer ciertos delitos. La suplantación de identidad, la extorsión, el ciberbullying, la violencia digital, la difusión de información falsa, la manipulación de pruebas o la vulneración de la privacidad pueden tener un impacto mucho más peligroso cuando se llevan a cabo a través del uso de sistemas automatizados o contenidos sintéticos. En consecuencia, el problema no es únicamente el hecho de que existan conductas ilícitas y punibles, sino que medie la tecnología, la cual incrementa el engaño, dificulta la identificación de la autoría y multiplica el daño producido.

La confrontación entre las propiedades técnicas de los contenidos sintéticos y las normas penales ecuatorianas permitió llegar a la conclusión de que la inteligencia artificial debe considerarse como un medio de ejecución que puede incrementar la lesividad de ciertas conductas. Esta conclusión se diferencia del marco teórico, ya que no únicamente determina las prestaciones de la tecnología, sino que comprueba la incidencia de esta en la aplicación de los tipos penales vigentes en la actualidad.

Peligros jurídicos y sociales de la suplantación a través de inteligencia artificial

La suplantación a través de la inteligencia artificial es peligrosa porque permite extender el uso y la reproducción de datos íntimos y personales de la persona que sufre la suplantación, como su rostro, su voz, sus gestos, su imagen pública o su identidad digital. La suplantación a través de inteligencia artificial permite ir más allá de lo que puede alcanzar la suplantación tradicional. Esta última se limita, en general, a utilizar el nombre, los documentos, las cuentas o los datos de una persona, mientras que la suplantación mediante inteligencia artificial permite generar una representación audiovisual aparentemente real de la víctima.

Este tipo de conducta puede tener consecuencias realmente graves. En primer lugar, la dignidad y la honra de la persona se ven perjudicadas, ya que se pueden atribuir a esta expresiones o comportamientos que nunca realizó. En segundo lugar, su intimidad y su imagen social se ven afectadas, toda vez que se utilizan características personales sin el consentimiento de la persona afectada. En tercer lugar, se pueden ocasionar perjuicios patrimoniales, laborales, emocionales o familiares, en razón de que la persona está expuesta a situaciones de chantaje, denigración, acoso o manipulación. En cuarto y último lugar, se puede afectar a la administración de justicia si los deepfakes se utilizan como prueba falsa o como un método para poner en cuestión la veracidad de una prueba verdadera.

La clasificación de las fuentes analizadas permitió deducir cuatro ámbitos de afectación: los derechos de la personalidad; el patrimonio y las relaciones laborales o familiares; la

confianza pública en los contenidos digitales; y la administración de justicia. Este hallazgo establece que la mala utilización de una misma creación sintética puede afectar simultáneamente varios bienes jurídicos. De ahí que la suplantación de la persona a través de la inteligencia artificial no pueda entenderse como una tipología idéntica a los delitos que ya se encuentran previstos. La peligrosidad de esta actividad alcanzaría un umbral mayor cuando se combinan la creación de contenido, la suplantación, su difusión pública y el propio hecho de que resulte muy difícil demostrar técnicamente la alteración realizada.

Pero el estudio también mostró que no toda creación o modificación digital debe reconocerse como una conducta delictiva. Para determinar la posible existencia de responsabilidad, hay que tener en cuenta la intención del autor, el consentimiento de la persona suplantada, la finalidad del contenido, el medio de divulgación, así como el daño ocasionado. Este descubrimiento permite distinguir entre los usos legítimos de la tecnología y aquellos que ofrecerían una razón para proceder a una intervención de orden penal. Igualmente, el equipo investigador evidenció que la norma ecuatoriana no dice de manera explícita cuándo comienza la relevancia penal, ya sea desde la elaboración de los contenidos, desde su distribución o desde la producción del daño. Esta situación impide establecer diferencias jurídicas entre las distintas fases de elaboración, posesión, publicación y utilización del material sintético.

Análisis del marco normativo

En Ecuador, la Constitución establece que existen determinados derechos que el uso malicioso de deepfakes puede vulnerar, como son la honra, el buen nombre, la imagen, la intimidad, la protección de datos de carácter personal, el debido proceso y la seguridad jurídica (Asamblea Constituyente, 2008). Los derechos pueden sufrir vulneración cuando se usa la identidad digital de una persona para atribuirle actos, expresiones o situaciones que no se han producido. La revisión constitucional da cuenta de que la problemática no se refiere a un solo derecho, en tanto la creación y difusión de un contenido sintético pueden comprometer simultáneamente la identidad, la intimidad, la honra, la imagen y la protección de los datos personales.

Si dicho contenido se incorpora en el marco de un proceso judicial, también pueden comprometer otros derechos o principios fundamentales, como el debido proceso y la seguridad jurídica. El Código Orgánico Integral Penal cuenta con algunos tipos penales que pueden hacerse parcialmente aplicables a estas conductas (Asamblea Nacional del Ecuador, 2014). El artículo 178, por ejemplo, impone pena de prisión a quien acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio, vídeo u objetos postales sin el consentimiento correspondiente o sin la autorización legal respectiva.

El artículo 179 regula la revelación del secreto; el artículo 212 establece la suplantación de la identidad; y los artículos 230, 232 y 234 tipifican conductas relacionadas con la interceptación ilegal de datos, los ataques contra la integridad de los sistemas informáticos y el acceso a sistemas sin consentimiento. El artículo 234.1 tipifica la falsificación informática en el sentido de que se producen o alteran datos con la intención de que sean utilizados como auténticos (Asamblea Nacional del Ecuador, 2014).

Sin embargo, estas disposiciones no tipifican expresamente la creación, difusión o utilización maliciosa de los deepfakes, por lo que su aplicación dependería de que la conducta se adecue a los elementos de un tipo ya existente. Esto puede causar problemas, especialmente cuando la lesión afecta los derechos, la imagen, la reputación o la identidad de la víctima, pero no se relaciona con accesos ilegales a sistemas, con la divulgación de datos íntimos, con alguna forma de beneficio económico o con una relación jurídica concreta.

Tabla 1. *Aplicabilidad de los tipos penales del COIP frente a conductas con Deepfakes*

Artículo COIP	Bien jurídico protegido	Conducta típica	Aplicabilidad frente a deepfakes	Limitación detectada
Art. 178	Intimidad	Acceso, interceptación, grabación, reproducción o difusión de datos personales sin consentimiento	Aplicable cuando exista utilización o divulgación no autorizada de contenido íntimo	No cubre la creación del contenido sintético, solo su difusión
Art. 179	Secreto	Revelación de secreto	Aplicable cuando el deepfake revele información reservada	No aborda la manipulación audiovisual ni la suplantación
Art. 212	Identidad	Suplantación de identidad	Aplicable cuando el deepfake contenga elementos de suplantación	No regula la representación audiovisual sintética ni su difusión masiva
Art. 230	Sistemas informáticos	Interceptación ilegal de datos	Aplicable cuando se intercepten datos para crear el deepfake	No tipifica la creación ni la difusión del contenido
Art. 232	Sistemas informáticos	Ataques contra la integridad de sistemas	Aplicable cuando se vulneren sistemas para obtener material audiovisual	No cubre la manipulación posterior del material
Art. 234	Sistemas informáticos	Acceso sin consentimiento	Aplicable cuando se acceda a sistemas para extraer material	No regula el uso del material extraído para fines ilícitos

Art. 234.1	Falsificación informática	Producción o alteración de datos para uso como auténticos	Aplicable cuando los datos falsificados se utilicen como auténticos	No abarca la difusión pública ni el daño a la honra o la imagen

Nota. Fuente: Elaboración propia con base en el análisis del Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014).

A partir de la confrontación individual de cada uno de los artículos estudiados, se obtuvo la siguiente relación: se puede aplicar el artículo 178 cuando haya una utilización o una divulgación no autorizada de contenido que pertenece al ámbito íntimo; el artículo 212 puede aplicarse cuando haya una acción que contenga los elementos constitutivos del delito de suplantación de identidad; y el artículo 234.1 puede aplicarse cuando los datos falsificados se utilicen como auténticos dentro de una relación jurídica. Sin embargo, ninguna de estas reglas alcanza por sí sola a comprender los diferentes modos de creación y difusión malintencionada de contenido sintético.

El principal hallazgo normativo consiste en que el COIP protege ciertos bienes jurídicos que los deepfakes vulneran, pero no reconoce expresamente los aspectos técnicos y perjudiciales de esta práctica. Así, la insuficiencia no se encuentra en la ausencia de normas, sino en su cobertura fragmentada y supeditada a los elementos típicos de delitos previstos para otras formas de conducta. La Tabla 1 sintetiza la aplicabilidad de cada tipo penal frente a conductas con deepfakes.

Análisis doctrinario

La revisión doctrinal cumplió la función de base hermenéutica y no constituyó un resultado independiente del trabajo. Por tal razón, en este apartado únicamente se muestran las categorías obtenidas de las fuentes, mientras que la confrontación específica con los autores se reserva para la discusión. La doctrina analizada permite vislumbrar hasta tres categorías aplicables al ordenamiento jurídico ecuatoriano: (i) la posible afectación de la privacidad, la seguridad y la confianza pública; (ii) las dificultades de adecuación de las conductas relacionadas con los deepfakes a los tipos penales tradicionales; y (iii) la complejidad técnica de la evidencia digital (Kerr, 2007; Miró Llinares, 2018; Chesney y Citron, 2019; UNODC, 2021).

A partir de estas categorías, el estudio analiza su aplicación al ordenamiento jurídico ecuatoriano, hasta llegar a los siguientes postulados: la afectación a la víctima no es la única consecuencia, dado que la circulación de contenidos cuya veracidad resulta difícil de probar podría debilitar la confianza social en las evidencias audiovisuales. Por otra parte, la comparación con el COIP permite determinar que las figuras de violación a la intimidad, suplantación de identidad y falsificación informática ofrecen respuestas parciales frente a ciertos aspectos del proceso de creación, distribución y uso malicioso de deepfakes.

También, en materia probatoria, se establece que una investigación penal relacionada con los deepfakes probablemente deba comprender el examen del archivo digital, sus metadatos, la búsqueda de los archivos originales y de las posibles alteraciones producidas desde su origen, la trazabilidad de la difusión y la cadena de custodia de la prueba. Esto se debe a que el contenido por sí solo no permite concluir si es un archivo auténtico, un archivo editado convencionalmente o un archivo generado mediante inteligencia artificial.

De esta manera, el resultado doctrinal permite dar cuenta de la insuficiencia parcial de los tipos penales tradicionales, la probable afectación simultánea de varios derechos y la complejidad técnica de la prueba digital. La comparación específica entre los planteamientos de cada autor se deja para la parte de discusión, con la finalidad de no repetir sus contribuciones doctrinales.

Análisis jurisprudencial

No se encontró una línea jurisprudencial ecuatoriana explícita acerca de delitos cometidos mediante deepfakes. La revisión documental tampoco permitió identificar resoluciones que determinen criterios para la valoración de contenidos audiovisuales generados o manipulados con inteligencia artificial, la comprobación de su autenticidad y la atribución de responsabilidad sobre su creación y difusión. A pesar de la posibilidad de que existan resoluciones sobre delitos informáticos, atentados contra la intimidad o suplantación de identidad, estas no recogen la dificultad evidente que presentan los deepfakes.

La falta de jurisprudencia genera incertidumbre entre fiscales, jueces, defensores y peritos, al no ofrecer pautas para distinguir entre contenido auténtico, contenido comúnmente editado y contenido sintético. El hallazgo jurisprudencial solo tiene sentido si se entiende dentro de los límites de la búsqueda documental que el equipo realizó. No se sostiene que en Ecuador no se hayan presentado hechos relacionados con contenidos sintéticos, sino que simplemente no se pudo identificar una línea de decisiones que estuviera suficientemente consolidada y fuera accesible como para determinar el tratamiento judicial que se otorga a estas conductas.

También se aprecia que la falta de precedentes o de decisiones judiciales dificulta establecer el nivel de certeza que debe alcanzar una pericia informática, la serie de elementos necesarios para atribuir la elaboración del contenido a una persona y la manera de resolver los cuestionamientos sobre la autenticidad de una prueba audiovisual. Por lo tanto, el análisis manifiesta la necesidad de establecer bases técnicas y jurídicas respecto de la prueba digital, la pericia informática y la responsabilidad penal en entornos de inteligencia artificial.

Identificación del problema jurídico

El problema jurídico más destacado que ha podido identificarse es que el ordenamiento penal ecuatoriano contiene algunas disposiciones generales, pero no tiene un régimen que regule específicamente a los deepfakes. Lo anterior puede generar vacíos de tipicidad si la conducta no encaja totalmente en la violación a la intimidad, la suplantación de identidad, la falsificación informática o el acceso no consentido a sistemas informáticos. El asunto no se limita a que no esté incluida la palabra deepfakes en el COIP. La cuestión central es que las normas actuales examinan la intimidad, la identidad, los sistemas informáticos y la falsificación de los datos de manera aislada, cuando el contenido sintético puede abarcar de forma conjunta toda esta serie de elementos.

Asimismo, fueron evidentes los problemas en el marco procesal vinculados a la prueba digital, dado que los deepfakes se pueden utilizar como prueba falsa o como mecanismo para negar la veracidad de una prueba verdadera. A esto se suman las complicaciones para atribuir responsabilidad penal, las cuales pueden derivarse del uso de cuentas falsas, servicios de anonimización, redes privadas virtuales o plataformas extranjeras. El análisis permitió establecer cuatro dimensiones del problema jurídico: la primera es normativa, en razón de la inexistencia de una normativa específica,

Mientras que, la segunda es probatoria, por la dificultad para establecer la autenticidad del material; la tercera es procesal, debido a las dificultades para obtener, preservar y valorar la prueba; y la cuarta es jurisdiccional, por la posibilidad de que los servidores, las plataformas o los autores se encuentren fuera del territorio ecuatoriano. La clasificación categorial es un hallazgo propio, porque se extrae de la sistematización de las normas, de las fuentes doctrinales y de los documentos institucionales revisados.

Marco legal aplicable

El marco jurídico aplicable se encuentra formado principalmente por la Constitución de la República del Ecuador y el Código Orgánico Integral Penal (Asamblea Nacional del Ecuador, 2014). La Constitución protege derechos como la honra, la imagen, la intimidad, la protección de datos personales, el debido proceso y la seguridad jurídica Asamblea Constituyente. (2008). Estas garantías pueden sufrir afectación cuando se producen o distribuyen deepfakes relacionados con una persona. En el Código Orgánico Integral Penal del Ecuador, los artículos 178, 179 y 212 pueden resultar aplicables en circunstancias concretas relacionadas con la intimidad, la información personal y la suplantación de la identidad de las personas (Asamblea Nacional del Ecuador, 2014).

Los artículos 230, 232, 234 y 234.1, por su parte, pueden resultar aplicables en los casos donde se produzcan la interceptación ilegal de datos, los ataques a los sistemas de información, el acceso sin consentimiento o la falsificación informática (Asamblea Nacional del Ecuador, 2014). No obstante, el análisis concluyó que dichos artículos solo pueden aplicarse cuando la conducta cumpla todos los elementos del tipo delictivo recogido en cada artículo. La utilización de la inteligencia artificial no sustituye la

comprobación del acceso no autorizado, la divulgación de datos personales, la suplantación de identidad, la falsificación de datos ni el resto de los elementos requeridos por la ley.

El ordenamiento jurídico ecuatoriano no menciona expresamente los deepfakes ni regula la manipulación audiovisual o sonora realizada mediante inteligencia artificial. Tampoco incluye un concepto de contenido sintético en su articulado ni asigna a ese tipo de contenido obligaciones para su identificación. De este modo, las disposiciones actuales son parcialmente aplicables, pero no proporcionan una respuesta clara a conductas dañinas que afectan la imagen, la reputación o la identidad y que no encajan en los tipos analizados.

En síntesis, los resultados muestran que el ordenamiento jurídico ecuatoriano contiene algunas normas que, en ciertos casos, pueden aplicarse a los deepfakes, aunque no de forma integral. La falta de una regulación genera inseguridad jurídica, produce dificultades probatorias y dificulta llevar a cabo la persecución de la creación, difusión y uso malicioso del contenido sintético. Los resultados de la investigación se pueden resumir en cuatro elementos: la aplicación fragmentada y parcial de los tipos penales existentes en el ordenamiento jurídico ecuatoriano; la falta de regulación específica de la información sintética; la falta de criterios jurisprudenciales comunes para resolver los conflictos que puedan presentarse; y las dificultades técnicas para obtener, conservar y valorar las evidencias digitales. Estos resultados constituyen la base que se contrasta posteriormente con la doctrina, el derecho comparado y las iniciativas legislativas.

Discusión

Los resultados de la investigación confirman que el derecho penal ecuatoriano enfrenta dificultades significativas para responder a los delitos cometidos mediante inteligencia artificial, en especial aquellos vinculados al uso de deepfakes. El problema no se limita a la aparición de una nueva herramienta tecnológica, sino que evidencia la emergencia de conductas capaces de afectar simultáneamente varios bienes jurídicos protegidos. Un mismo contenido sintético puede comprometer la identidad, la imagen, la intimidad, la reputación y la autenticidad de la información digital de una persona, mientras que la normativa actual protege estas cuestiones por separado. Esta fragmentación normativa constituye el eje central de la discusión que se desarrolla a continuación.

En primer lugar, los hallazgos se alinean con lo que Chesney y Citron (2019) establecieron al señalar que los deepfakes representan una amenaza para la privacidad, la seguridad, la democracia y la confianza pública. Esta afirmación resulta plenamente aplicable al contexto ecuatoriano, puesto que la ausencia de un tipo penal específico dificulta la persecución de conductas que afectan la imagen o la identidad de la víctima mediante contenidos audiovisuales manipulados. No obstante, el análisis permite

advertir que la sola incorporación del término deepfakes al COIP no resolvería el problema. Resulta necesario definir la intención ilícita, la falta de consentimiento, la finalidad del contenido y el perjuicio concreto, a fin de distinguir los usos legítimos de aquellos que justifican la intervención penal.

En segundo lugar, Miró Llinares (2018) sostiene que la inteligencia artificial genera problemas al momento de circunscribir la conducta delictiva dentro del derecho penal, dado que muchas acciones tecnológicas no encajan con facilidad en las categorías tradicionales. Esta idea se refleja con claridad en los resultados del presente estudio, ya que el COIP contiene normas sobre violación a la intimidad, suplantación de identidad y falsedad informática, pero ninguna aborda de manera directa la creación, difusión o uso malicioso de deepfakes. En consecuencia, las disposiciones vigentes permiten enfrentar determinados resultados lesivos, pero no ofrecen una regulación integral del proceso completo de generación y utilización del contenido sintético.

Desde la perspectiva probatoria, Kerr (2007) vincula la prueba digital con su carácter volátil, modificable y dependiente de herramientas técnicas. Esta cuestión adquiere especial relevancia cuando se trata de delitos relacionados con inteligencia artificial, porque no basta con aportar un vídeo o un audio al proceso penal. El investigador debe acreditar si el contenido sufrió manipulación, quién lo generó, cómo se difundió y cuál era el objetivo de su utilización. Por lo tanto, el vacío detectado no solo es normativo, sino también procesal y pericial, ya que Ecuador carece de un protocolo técnico definido para obtener, conservar y valorar la prueba digital derivada de contenidos sintéticos.

Además, la literatura reciente ha demostrado que los deepfakes constituyen una amenaza epistémica para la sociedad, en tanto erosionan la capacidad de los individuos para distinguir entre contenidos auténticos y fabricados. Fallis (2021) argumenta que esta tecnología debilita los fundamentos del conocimiento compartido y puede generar un escenario de escepticismo generalizado respecto de la evidencia audiovisual. Vaccari y Chadwick (2020) comprobaron empíricamente que los vídeos políticos sintéticos alteran la percepción de la realidad y reducen la confianza en las noticias. Estos hallazgos refuerzan la urgencia de una respuesta jurídica que proteja no solo a la víctima individual, sino también la integridad del ecosistema informativo.

En el ámbito del derecho comparado, la Unión Europea aprobó el Reglamento (UE) 2024/1689, que establece obligaciones de transparencia para los contenidos generados o manipulados mediante inteligencia artificial, incluidos los deepfakes. Dicha norma exige que los proveedores de sistemas de IA informen a los usuarios cuando el contenido haya sufrido alteraciones artificiales, en particular cuando pueda inducir a error sobre su autenticidad (Parlamento Europeo y Consejo de la Unión Europea, 2024). Este marco regulatorio demuestra que otros ordenamientos jurídicos ya reconocieron la necesidad de abordar de forma específica los riesgos derivados de los contenidos sintéticos, mientras que Ecuador aún mantiene una respuesta de carácter general.

En América Latina, Chile promulgó la Ley 21.459 en 2022, la cual modernizó la legislación sobre delitos informáticos y la adecuó al Convenio de Budapest. Si bien dicha norma no contempla expresamente los deepfakes, sirve como referente regional para la actualización de los tipos penales frente a las nuevas formas de criminalidad digital (Biblioteca del Congreso Nacional de Chile, 2022). En contraste, Ecuador mantiene una regulación penal más general y fragmentada. Esta revisión no debería limitarse a insertar términos vinculados a una tecnología determinada, dado que la tecnología evoluciona con rapidez. Lo más adecuado consiste en formular disposiciones que se concentren en la manipulación intencionada de la identidad y del contenido digital.

En Estados Unidos, algunos estados han desarrollado respuestas específicas ante el uso malicioso de deepfakes, en especial en el ámbito electoral. Un ejemplo relevante es Texas, cuya normativa contempla sanciones para la difusión de vídeos falsos que pretendan influir en procesos electorales concretos (Texas Constitution and Statutes, 2025). Esta diferencia normativa indica que Ecuador se encuentra en una fase inicial de desarrollo regulatorio frente a este fenómeno. Sin embargo, las soluciones extranjeras no resultan trasladables de forma mecánica, pues cada ordenamiento posee principios constitucionales, formas de estructuración penal y necesidades sociales diferentes. Su mayor contribución radica en ofrecer alternativas que el legislador ecuatoriano debe analizar y evaluar según la realidad jurídica nacional.

Respecto a los proyectos legislativos ecuatorianos, la Asamblea Nacional registra el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador, cuyo contenido pretende avanzar en la elaboración de un marco regulatorio sobre el uso de la IA en el país. También figura el Proyecto de Ley Orgánica que regula el uso de simulaciones de imágenes, voces, audios y vídeos de personas generados a partir de inteligencia artificial. Esta segunda propuesta se vincula de manera más directa con el objeto de la presente investigación, dado que tiene por propósito regular el uso de contenidos sintéticos (Asamblea Nacional del Ecuador, 2026). No obstante, la mera presentación de estas iniciativas no elimina las dificultades identificadas.

La existencia de las iniciativas legislativas resulta insuficiente para eliminar el vacío normativo previamente señalado. Mientras no exista una disposición que regule de manera expresa la creación, difusión y utilización maliciosa de deepfakes, el sistema de justicia penal dependerá de figuras generales que pueden resultar insuficientes frente a las particularidades de cada conducta. Esta necesidad de actualización no debe entenderse como una ampliación indiscriminada del poder punitivo. Por el contrario, una posible reforma debe respetar los principios de legalidad, proporcionalidad y mínima intervención penal, a fin de que la sanción se centre en las conductas dirigidas intencionalmente a ocasionar un daño jurídicamente relevante.

La discusión también permite afirmar que Ecuador requiere una actualización del marco normativo que sea equilibrada. La respuesta jurídica no debería limitarse a la creación

de un nuevo delito, dado que la persecución penal continuaría insuficiente sin protocolos periciales, sin capacitación de fiscales, jueces, defensores y peritos judiciales, y sin mecanismos de cooperación con las plataformas digitales y las autoridades de otros países. Organismos internacionales como la UNODC han subrayado que los delitos cibernéticos exigen respuestas integrales que combinen la reforma legislativa con el fortalecimiento institucional y la cooperación transnacional (UNODC, 2021). De igual forma, la UNESCO ha recomendado que los Estados desarrollen marcos éticos y jurídicos que regulen el uso de la inteligencia artificial y protejan los derechos fundamentales (UNESCO, 2021).

En síntesis, una reforma penal parcial, acompañada de medidas procesales e institucionales, permitiría consolidar la seguridad jurídica, proteger derechos fundamentales y ofrecer una capacidad de respuesta organizada del sistema de justicia frente a la criminalidad digital contemporánea. Los hallazgos de esta investigación evidencian que el ordenamiento jurídico ecuatoriano necesita transitar desde una regulación fragmentada hacia un marco integral que reconozca las particularidades técnicas de los contenidos sintéticos. Dicha transición debe incorporar la tipificación específica de conductas, la definición de protocolos probatorios, la formación de operadores jurídicos y el establecimiento de mecanismos de cooperación internacional que permitan enfrentar un fenómeno que, por su naturaleza tecnológica, trasciende las fronteras nacionales.

Conclusiones

La presente investigación confirma la existencia de un vacío normativo en el ordenamiento jurídico penal ecuatoriano frente a los delitos cometidos mediante inteligencia artificial, en especial aquellos relacionados con el uso, creación o difusión maliciosa de deepfakes. El Código Orgánico Integral Penal contiene disposiciones vinculadas a la violación de la intimidad, la revelación de información personal, la suplantación de identidad y la falsificación informática; sin embargo, dichas normas solo admiten una aplicación parcial, puesto que no describen de manera expresa la manipulación audiovisual o sonora que la inteligencia artificial produce. Esta insuficiencia normativa constituye el hallazgo central del estudio.

En relación con el primer objetivo específico, el análisis demostró que a través de los deepfakes resulta posible cometer diversas conductas lesivas: la suplantación de identidad, la afectación a la honra, la vulneración de la intimidad, el acoso, la extorsión, la difusión de información falsa y la manipulación de pruebas digitales. Los hallazgos evidencian que la inteligencia artificial no opera únicamente como una herramienta tecnológica, sino también como un medio que incrementa la gravedad de la lesión, dado

su potencial para simular con elevado realismo rostros, voces, gestos y conductas de una persona.

Respecto del segundo objetivo específico, el estudio concluyó que el COIP adolece de limitaciones estructurales para responder de manera adecuada a esta forma de delincuencia digital. El problema no radica en la inexistencia de normas penales, sino en la ausencia de una tipificación específica que permita sancionar con claridad la creación, circulación y uso malicioso de contenidos sintéticos. Esta circunstancia puede generar vulneraciones a la seguridad jurídica, interpretaciones forzadas de los tipos penales vigentes y dificultades en la aplicación del principio de legalidad cuando la conducta no coincide plenamente con las figuras penales clásicas.

En cuanto al tercer objetivo específico, la investigación determinó que los delitos cometidos mediante deepfakes presentan dificultades probatorias de considerable magnitud. La prueba digital puede sufrir manipulación, replicación, eliminación o difusión a través de plataformas ubicadas en el extranjero. Esta situación dificulta la identificación del autor, la conservación de la cadena de custodia, la verificación de autenticidad y la valoración del contenido audiovisual ante el tribunal. Por consiguiente, el vacío detectado no solo es normativo, sino también procesal y pericial, ya que la persecución penal requiere herramientas técnicas y criterios especializados para determinar si un contenido fue generado o manipulado mediante inteligencia artificial.

En lo concerniente al cuarto objetivo específico, el análisis permitió establecer que Ecuador necesita criterios jurídicos de actualización normativa y de fortalecimiento institucional. La reforma del COIP debe integrar de forma expresa las conductas relacionadas con los deepfakes o contenidos sintéticos utilizados para fines ilícitos, pero con respeto a los principios de legalidad, proporcionalidad y mínima intervención penal. De igual forma, resulta imprescindible el establecimiento de protocolos especializados de investigación digital, la capacitación de fiscales, jueces, defensores y peritos, así como la creación de mecanismos de cooperación internacional para combatir delitos que, por su carácter tecnológico, pueden trascender las fronteras nacionales.

En definitiva, la investigación corrobora que la rápida evolución de la inteligencia artificial ha sobrepasado la capacidad de respuesta del sistema penal ecuatoriano para abordar los delitos que involucran tecnologías de deepfakes. Esta desactualización normativa afecta la eficacia de la investigación penal, limita la protección de los derechos fundamentales y genera nuevas dificultades para la administración de justicia.

Por lo tanto, resulta imprescindible una actualización normativa integral que permita una adecuada tipificación de las conductas, la fijación de criterios claros para la evaluación de la evidencia digital y la promoción de la capacitación continua de los operadores del sistema de justicia. Futuras investigaciones podrán profundizar en el análisis de casos registrados a nivel nacional y en la comparación de experiencias

regulatorias que permitan elaborar un modelo normativo acorde con la realidad ecuatoriana.

Acerca de

Contribución de los autores: Los autores contribuyeron a la conceptualización del estudio, al desarrollo metodológico, al análisis e interpretación de los datos, a la redacción del manuscrito y a la revisión crítica de su contenido intelectual. Todos los autores aprobaron la versión final para su publicación.

Financiamiento: Los autores declaran que no recibieron financiamiento para esta investigación.

Conflicto de interés: Los autores declaran no tener conflicto de intereses para la publicación del presente artículo científico.

Certificación ética: El protocolo del presente estudio fue sometido a revisión y aprobado por el Comité de Ética en Investigación de la Universidad, en cumplimiento de los principios éticos y normativas institucionales aplicables.

Referencias

Asamblea Constituyente. (2008). *Constitución de la República del Ecuador.* Registro Oficial No. 449. https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal. Registro Oficial Suplemento No. 180.* https://www.gob.ec/sites/default/files/regulations/2020-11/DOCUMENTO_C%C3%93DIGO-ORG%C3%81NICO-INTEGRAL-PENAL-COIP_0.pdf

Asamblea Nacional del Ecuador. (2024). *Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador.* https://www.asambleanacional.gob.ec/es/multimedios-legislativos/97303-proyecto-de-ley-organica-de-regulacion

Asamblea Nacional del Ecuador. (2026). *Proyecto de Ley Orgánica que regula el uso de las simulaciones de imágenes, voces, audio y video de personas generadas por inteligencia artificial.* https://www.asambleanacional.gob.ec/es/node/115325

Biblioteca del Congreso Nacional de Chile. (2022). *Ley N.º 21.459: Establece normas sobre delitos informáticos, deroga la Ley N.º 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.* LeyChile. https://www.bcn.cl/leychile/navegar?idNorma=1177743

Chesney, B., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Fallis, D. (2021). The epistemic threat of deepfakes. *Philosophy & Technology, 34*(4), 623–643. https://doi.org/10.1007/s13347-020-00419-2

Kerr, O. S. (2007). *Digital evidence and the new criminal procedure.* In J. M. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman, & T. Zarsky (Eds.), Cybercrime: Digital cops in a networked environment (pp. 221–246). New York University Press. https://doi.org/10.18574/nyu/9780814739334.003.0013

Miró Llinares, F. (2018). Inteligencia artificial y justicia penal: Más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, 20, 87–130. https://revistas.uned.es/index.php/RDPC/article/view/22235

Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).* Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es

Texas Constitution and Statutes. (2025). *Election Code, Chapter 255: Regulating political advertising and campaign communications.* https://statutes.capitol.texas.gov/?chapter=EL.255&code=EL&tab=1

UNESCO. (2021). *Recomendación sobre la ética de la inteligencia artificial.* https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence

United Nations Office on Drugs and Crime [UNODC]. (2021). *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021 (UNODC/CCPCJ/EG.4/2021/2).* https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1). https://doi.org/10.1177/2056305120903408