Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 6 – Núm. 2 / Julio – Diciembre – 2025

La ausencia de respuesta penal frente al uso doloso de la inteligencia artificial

The absence of criminal responsibility for the fraudulent use of artificial intelligence

A ausência de responsabilidade criminal pelo uso fraudulento da inteligência artificial

Vera-Ruiz, Bryan Anibal
Universidad Bolivariana del Ecuador
baverar@ube.edu.ec
https://orcid.org/0009-0003-5233-7924

García-Segarra, Holger Geovannny
Universidad Bolivariana del Ecuador
hggarcias@ube.edu.ec
https://orcid.org/0009-0009-2499-762X

DOI / URL: https://doi.org/10.55813/gaea/ccri/v6/n2/1189

Como citar:
Vera-Ruiz, B. A., & García-Segarra, H. G. (2025). La ausencia de respuesta penal frente al uso doloso de la inteligencia artificial. *Código Científico Revista De Investigación, 6*(2), 228–255.

Recibido: *02/11/2025* ***Aceptado:*** *01/12/2025* ***Publicado:*** *31/12/2025*

Resumen
El uso doloso de la inteligencia artificial (IA) en los procesos electorales presidenciales ha transformado las campañas en escenarios de manipulación, desinformación y violencia política, especialmente durante los comicios celebrados en Ecuador durante los años de 2021 y 2023. Este fenómeno incluye la difusión masiva de «*deepfakes*», imágenes sexualizadas y noticias falsas dirigidas contra figuras públicas, y ciudadanos comunes, exacerbando vulneraciones a derechos como la imágen, la honra y la participación política. En un contexto global, este uso indiscriminado de la IA, no solo se limita a un perjuicio de la imágen o la honra, sino que además es utilizado potencialmente para hacer daño bajo el anonimato, como una herramienta *replicativa y generativa de datos* que busca la impunidad. En la actualidad, el marco jurídico ecuatoriano carece de tipificaciones específicas y mecanismos procesales eficaces para abordar esta problemática, lo que genera impunidad y dificulta la reparación a las víctimas. Esta investigación propone una reforma normativa para crear un tipo penal autónomo incorporado al título IV del COIP, que regule los delitos informáticos, específicamente como nuevo conjunto de artículos derivado del 234 que sancione la manipulación digital dolosa mediante IA; de tal forma que se prevenga a la sociedad ante el uso indiscriminado de estas nuevas tecnologías con fines dolosos, garantizando así el respecto de los derechos fundamentales.
Palabras clave: inteligencia artificial, deep fakes, manipulación digital, derecho a la imágen, vacío normativo, impunidad, dolo.

Abstract
The malicious use of artificial intelligence (AI) in presidential electoral processes has transformed political campaigns into arenas of manipulation, disinformation, and political violence, particularly during the elections held in Ecuador in 2021 and 2023. This phenomenon includes the widespread dissemination of deepfakes, sexualized images, and fabricated news targeting both public figures and ordinary citizens, thereby intensifying violations of rights such as personal image, honor, and political participation. In a global context, the indiscriminate use of AI extends beyond harm to reputation; it also enables anonymous aggression through replicative and generative data tools designed to evade accountability. Currently, the Ecuadorian legal framework lacks specific criminal classifications and effective procedural mechanisms to address this issue, resulting in impunity and hindering adequate redress for victims. This research proposes a legal reform to create an autonomous criminal offense within Title IV of the COIP, regulating cybercrimes specifically as a new set of provisions derived from Article 234 to penalize the intentional digital manipulation carried out through AI. Such reform would help safeguard society from the improper use of emerging technologies for malicious purposes, thereby ensuring the protection of fundamental rights.
Keywords: artificial intelligence, deepfakes, digital manipulation, right to image, regulatory gap, impunity, intent.

Resumo
O uso malicioso da inteligência artificial (IA) nos processos eleitorais presidenciais transformou as campanhas políticas em arenas de manipulação, desinformação e violência política, particularmente durante as eleições realizadas no Equador em 2021 e 2023. Esse fenómeno inclui a disseminação generalizada de deepfakes, imagens sexualizadas e notícias fabricadas visando tanto figuras públicas quanto cidadãos comuns, intensificando assim as violações de direitos como imagem pessoal, honra e participação política. Num contexto

global, o uso indiscriminado da IA vai além dos danos à reputação; também permite agressões anónimas por meio de ferramentas de dados replicativas e generativas projetadas para evitar a responsabilização. Atualmente, o quadro jurídico equatoriano carece de classificações criminais específicas e mecanismos processuais eficazes para lidar com essa questão, resultando em impunidade e dificultando a reparação adequada às vítimas. Esta investigação propõe uma reforma jurídica para criar um crime autónomo no Título IV do COIP, regulamentando os crimes cibernéticos especificamente como um novo conjunto de disposições derivadas do Artigo 234 para penalizar a manipulação digital intencional realizada por meio da IA. Tal reforma ajudaria a proteger a sociedade do uso indevido de tecnologias emergentes para fins maliciosos, garantindo assim a proteção dos direitos fundamentais.
Palavras-chave: inteligência artificial, deepfakes, manipulação digital, direito à imagem, lacuna regulatória, impunidade, intenção.

Introducción

En el contexto ecuatoriano, la globalización ha permitido avances tecnológicos casi impensables; las plataformas digitales dejaron de ser instancias de entretenimiento y aprendizajes y se transformaron en espacios de confrontación digital, moduladas por nuevas formas de detrimento a los derechos de las personas; con la creación de las deepfakes, videos con rostros y voces manipuladas, fotomontajes sexualizados y noticias falsas distribuidas en redes sociales y plataformas digitales, inclusive destinadas a desprestigiar e imputar delitos a los aspirantes políticos que son objeto de elecciones populares.

No solo las élites políticas o determinados personajes de alta exposición pública, como celebridades o influencers son víctimas de esta problemática, la cual se perfecciona día tras día debido a los constantes avances tecnológicos, sino cualquier ciudadano con identidad digital. Un ejemplo ilustrativo es el caso de la influencer manabita conocida como la «Chonera Bonita» (Televicentro, 2025), cuya intimidad fue violentada mediante la difusión en redes sociales a través de la creación de contenido sexual falso generado por un algoritmo de inteligencia artificial. En un contexto similar, el sistema educativo encendió las alarmas tras la circulación de contenido sexual creado con la identidad de menores de edad, presuntamente estudiantes y exalumnos de un reconocido colegio de la ciudad de Quito,

hecho que demuestra la extensión del fenómeno en distintos estratos de la sociedad ecuatoriana (Extra Digital, 2023).

En términos jurídicos, la teoría del Derecho Penal y Procesal Penal, estos acontecimientos presentan desafíos sin precedentes para la imputación de responsabilidad. En este caso, en escenarios inéditos, el iter criminis se difumina (Alonso & Sánchez, 2024). Este es un hecho lesivo verificable, es decir, contenido con apariencia delictiva que causa perjuicio real.

En primer lugar, el autor material o intelectual directo no siempre es identificable debido a la generación automática de contenido, anonimato en línea, manipulación de direcciones IP y replicación exponencial en redes distribuidas (Crawford, 2018). En segundo lugar, los factores específicos de estilo de la cibernética en la dinámica de la comunicación no permiten proporcionar pruebas tecnológicas a priori irrefutables. Por lo tanto, estos delitos son una variante de delitos fantasmas (Borja V. , 2024).

Finalmente, a esta dificultad se agrega otra de naturaleza normativa pertinente. En el ordenamiento penal positivo ecuatoriano, existe una laguna en el tratamiento de delitos informáticos que sancione la creación y difusión de fakes news, que en la mayoría de casos son originados por el uso doloso de sistemas de IA (Alonso & Sánchez, 2024). Si bien el Capítulo Tercero (III) del Código Orgánico Integral Penal (en adelante COIP), tipifica conductas como la falsificación informática detallada en el art. 234 numeral 1; y, el hostigamiento digital establecido en el art. 154 numeral 2; lo hace sobre la base de que la voluntad humana se activa en esta comisión del ilícito (Código Orgánico Integral Penal [COIP], 2014).

Esta brecha jurídica se encuentra ligada con la ausencia de normas que regulen y límiten el desarrollo exponencial del uso doloso de las fakes news, prácticas que vulneran derechos y afectan a la honra de las personas. Por tanto, se requiere, una acción penal que

tenga como objetivo no solo la protección de datos e identidad digital contra estos sistemas generativos, o comúnmente denominados como inteligencia artificial IA, sino también garantizar el respeto a los derechos fundamentales y prevenir conductas dolosas. No obstante, aunque el Ecuador cuenta con la Ley Orgánica de Protección de Datos Personales, su aplicación en la práctica sigue siendo limitada, y en muchos casos inexistente, es decir, esta normativa no está diseñada para afrontar los problemas planteados por los algoritmos generativos en virtud de las nuevas tecnologías y peor aún, las consecuencias derivadas de su mal uso. Por citar un ejemplo, en los procesos electorales, ha quedado en evidencia que, los datos personales de los candidatos, activistas y ciudadanos pueden ser recopilados, almacenados, y procesados; en la mayoría de casos, son expuestos mediante el anonimato y difundidos con el fin de causar un perjuicio, usando la identidad digital, como ocurre en la mayoría de casos, para distorsionar, cambiar o modificar tal identidad, o los datos personales (voz, audio, imágen, etc), sin un consentimiento explícito y sin un mecanismo eficaz para regularlo, exponiendo los datos biométricos, patrones de voz e imágenes a un uso indebido.

Tomando como base el derecho comparado, solo aquello producido por seres humanos puede disfrutar de protección legal en términos de «autoría», así como de ser considerado un producto de creación. En consecuencia, si el contenido, ya sea en forma de imágen, audio o video (datos en general), ha sido creado en su totalidad por IA sin prácticamente ninguna creatividad humana involucrada, no hay autor legalmente corroborado desde un enfoque de propiedad intelectual y autoría delictiva (Baños, 2024).

En tal sentido, la parte probatoria que no es tema central de este trabajo, pero si relevante, presenta dificultades para su procesamiento técnico, pues genera un entorno de incertidumbre, dado que a pesar de que el COIP permite reconocer el contenido digital como prueba admisible, de acuerdo al artículo 500 (Código Orgánico Integral Penal [COIP], 2014), exige protocolos de la cadena de custodia, integridad forense y autenticidad técnica, que se

tornan difícil cumplir cuando el contenido circula descontroladamente en las redes o ha sido manipulado con herramientas que no dejan rastro (Borja V. , 2024).

Esta nueva realidad implica repensar los conceptos clásicos del Derecho Penal, como la autoría, dolo, nexo de causalidad, imputabilidad, resultan limitados en un contexto de tecnología no previsto por el legislador y que permite que el infractor no esté conectado físicamente al delito (Malo & Lozano, 2024), (Crawford, 2018).

De esta manera, el presente estudio pretende avanzar no solo en la constatación de la afectación a derechos fundamentales como la imágen; también en la prevención y limitaciones del uso indiscriminado con fines dolosos de estas herramientas generativas, que en la mayoría de casos tiene como finalidad *lesionar un bien jurídico protegido, producto de la creación y difusión de las fakes news*; además, en la medida de los marcos interpretativos que permitan reconfigurar la respuesta estatal ante estos fenómenos emergentes (Giletta, Mercaú, Orden, & Villareal, 2020), (Gutiérrez & Abeliuk, 2022).

Metodología

El diseño de esta investigación se enmarca dentro del esquema exploratorio descriptivo de enfoque cualitativo; cuyo fin es conocer los efectos *jurídicos,* de la utilización de la inteligencia artificial en la intervención de la imágen, creación de datos y demás información potencialmente modificable de un ciudadano que goza de una identidad, pudiendo ser esta digital.

El principal método aplicado es el enfoque analítico y documental dogmático jurídico, que se complementa con métodos hermenéuticos, axiológicos y sistémicos (Secretaría de Marina, 2021). Debido a esta combinación metodológica, es posible realizar una lectura crítica de los elementos constitutivos de los delitos digitales en función de contextos de gran complejidad, como los que tienen por objeto de intervención, casos en los que los autores

supuestamente no pueden ser identificados materialmente, pues resulta casi «imposible», debido a la multiplicidad de copias y replicaciones del contenido.

Entre las técnicas utilizadas se encuentran la sistematización las siguientes normas legales vigentes; nacionales e internacionales, constitucional, penal, y demás concordantes; y, la revisión de casos mediáticos ocurridos en procesos electorales ecuatorianos durante los años 2021 a 2025, entre otros, cuyo objeto de crítica es el uso doloso de la IA.

En cuanto al universo de fuentes, este trabajo se basa en fuentes secundarias y reportes técnicos sobre el uso de IA con fines dolosos, en contextos electorales, etc, mediante el acceso a bases de datos especializadas, como Dialnet, Scielo, RedALyC, JSTOR, Google Scholar, y repositorios institucionales de universidades y centros de investigación; así como el uso de plataformas digitales como youtube.

En esta investigación jurídica, también se hace mención a informes oficiales de organismos como ONU, la OEA, la Corte Interamericana de Derechos Humanos, el Consejo Nacional Electoral del Ecuador, la Defensoría del Pueblo, entre otro, para la sustentación empírica de los casos analizados.

Resultados

El derecho a la imágen como derecho fundamental en entornos y la identidad digital

El derecho a la imágen se encuentra intrínsecamente enraizado en uno de los cimientos del sistema de derechos personalísimos, al ser compatible con la dignidad humana, la autonomía individual y la autodeterminación informativa (Mondria, 2023). Protege no solo la representación visual del cuerpo humano, sino cualquier exteriorización gráfica, fotográfica, videográfica que pueda atentar contra su integridad (Feria, 2022).

Cabe acotar que el derecho a la imágen, en la normativa del Ecuador, se encuentra establecido de forma expresa en el artículo 66, numeral 19, de la Constitución de la

República del Ecuador (Constitución de la República [CRE], 2008). Sin embargo, el entorno digital ha cambiado dramáticamente el alcance y la forma en que este derecho puede ser vulnerado.

La identidad digital puede definirse como el conjunto de datos o información recopilable de un individuo que reposa en internet y que le otorga características únicas. La reciente LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (Registro Oficial Suplemento 459 de 26-may.-2021), aunque tiene por objeto y busca garantizar la «protección de datos personales», presenta lagunas jurídicas, pues se limita a una protección de datos en sentido general y no en virtud de la prevención de delitos producto de la manipulación de estos datos, de allí la falta de una regulación que tenga como finalidad prevenir el uso indebido con fines dolosos creados por IA, así como al uso no autorizado de los mismos con fines dolosos.

Las plataformas digitales, el desarrollo de las redes sociales y, más recientemente, tecnologías basadas en inteligencia artificial generativa, cuyo producto son las deepfakes o clonación de voz o modelos text-to-video, han extendido las fronteras tradicionales del derecho a la imágen y han diversificado las formas de agresión simbólica posibles, muchas veces ambiguas al encajar bajo la clasificación «derecho a la imágen» (Priego, 2022).

Además, no solo se trata de la perturbación de la imágen personal, sino del uso indebido de los datos personales, ya que las tecnologías de inteligencia artificial detrás de los contenidos manipulados a menudo se basan en bases de datos injustificadas que pueden ser divisadas a través del rastreo a gran escala de la información digital. Aunque la Ley Orgánica de Protección de Datos Personales, firmada en 2021, protege el derecho de cada ser humano a la privacidad de los datos, el acceso y control sobre ellos, los mecanismos actuales son insuficientes para prevenir la extracción, almacenamiento y uso residual de esos datos

(sonidos o patrones biométricos), para el propósito de la manipulación política y violencia simbólica.

En particular, los deepfakes, han permitido la creación de contenido visual hiperrealista que puede alterar la apariencia, la voz y los gestos de una persona próxima, con o sin el consentimiento de ella, para fines tan disímiles como la sátira política y la pornografía no consensuada, la desinformación electoral (Montes, 2024).

En este sentido, el derecho a la imágen enfrenta un desafío doble: por un lado la rapidez, la dimensión cuantitativa y la anonimia en la que se expanden las imágenes manipuladas (fake news). Por otro lado, el fenómeno de la escala, el daño por una identidad alterada o descontextualizada no se circunscribe a un espacio privado e íntimo o público y local, sino que la representación de la víctima puede escalar globalmente en cuestión de segundos, multiplicando su daño (Borja C. , 2023).

A nivel procesal, esta situación constituye un desafío estructural a la hora de la acusación, dado que los contenidos son generados de manera automatizada y anónima, o en otras ocasiones a través de rusheos o de direcciones IP maquilladas, lo que hace prácticamente imposible deducir al autor material del delito (Giletta, Mercaú, Orden, & Villareal, 2020). Como consecuencia, se ven debilitadas las capacidades del sistema judicial de formular una acusación suprimida y de demostrar el nexo de causalidad entre el hecho y su responsable, repercutiendo tanto en el derecho al debido proceso como el derecho a la tutela judicial efectiva (Muñoz, 2024).

A pesar de que en Ecuador, el delito asociado al uso de la imágen personal viene regulado por figuras penales y procesales como la falsificación informática (artículo 234.1 Código Orgánico Integral Penal) y el hostigamiento digital (artículo 154.2) (Código Orgánico Integral Penal [COIP], 2014), problemas de inadecuación surgen para casos mucho más complejos de manipulación de la imagen personal a través del algoritmo. Así, por ejemplo,

no se ha previsto una tipificación específica del delito con relación a los actos de «creación, difusión y reproducción no consentida entre privados de las imágenes generadas por la inteligencia artificial, ni un protocolo para la adecuación de la prueba al tema» (Código Orgánico Integral Penal [COIP], 2014).

El desarrollo tecnológico lleva consigo una profunda transformación en las maneras en que los delitos se cometen, particularmente en el ámbito digital. A la fecha, uno de los mayores desafíos que se plantean tanto para el Derecho penal como para el Derecho procesal penal consiste en la dificultad de poder identificar y probar lo que, en un delito digital cometido con intervención de inteligencia artificial, se conoce como el iter criminis digital, desde la fase de su ideación hasta la consumación (Tarrillo, 2024).

Iter criminis digital y delitos sin autoría material directa

La problemática se vuelve compleja cuando los contenidos generados, como las fake images, audios o videos alterados, carecen de una «autoría humana material» directamente imputable; dificultando la atribución penal, y la comprobación del nexo causal (Devis, 2025), sobre todo porque el iter criminis, tradicionalmente, se constituía de un acto de voluntad humana que activaba la ejecución de un delito (Varona, 2024), sin embargo, en un marco digital, esta secuencia, aunque conserve validez no es totalmente humana.

En este orden de ideas, las fake news generadas mediante IA que simulan de manera hiperrealista rostros, voces o gestos de personas reales (deep fakes), sin su autorización o participación en la generación de tal contenido (Rouhiainen, 2018), no pueden ser legalmente atribuidos directamente a una persona (Ojeda, 2024), sobre todo cuando se usan para ellos direcciones IP enmascaradas.

En efecto, la ausencia de un sujeto pasivo deviene aún más grave en el ámbito penal, debido a que los principios de legalidad y responsabilidad personal exigen de un sujeto pasivo, sin embargo, en estos casos el autor se difumina en una red de automatismos,

servidores descentralizados y el espesor del anonimato digital (Solar, 2021). Como consecuencia de aquello, la víctima (mujeres, adolescentes, activistas, figuras políticas), sufren una grave afectación de su derecho al acceso a la justicia, la reparación integral y la garantía de no repetición, derechos consagrados en el bloque de constitucionalidad ecuatoriano, lo que se agrava ante la dificultad de ubicar el origen del contenido ilícito y, por ende, de activar mecanismos eficaces de persecución penal.

En particular, en la República del Ecuador, la IA se ha utilizado de manera significativa en escenarios políticos y electorales. La difusión de contenidos manipulados, incluyendo imágenes, audios o videos hiperrealistas que distorsionan la identidad o los mensajes de actores políticos, evidencian el riesgo que representas estas tecnologías cuando son utilizadas con fines de desinformación. Sin embargo, estos hechos rara vez derivan en un procedimiento judicial eficaz, principalmente porque no existe un marco normativo fuerte que tipifique estas conductas en el área penal y que a su vez, permita el tratamiento adecuado en la jurisdicción electoral.

Desde el punto de vista del Derecho Electoral, la utilización de sistemas de inteligencia artificial para alterar la imagen de los candidatos o crear información inexacta afecta de forma directa el principio de equidad en la contienda electoral, reconocido en el artículo 108 de la Constitución del Ecuador (Constitución de la República [CRE], 2008) y desarrollado a su vez, en el Código de la Democracia.

La revolución tecnológica, sin embargo, no ha estado acompañada por un desarrollo normativo equivalente, especialmente cuando se trata de los riesgos de la falsificación informática (Art. 234.1 COIP) cuando se utiliza como instrumento para la manipulación política, la difamación, el acoso o la violencia simbólica (Feria, 2022), dado que abarca la generación de datos no genuinos. Como resultado, en el caso del Ecuador, la desalineación entre la innovación tecnológica y la regulación legal ha creado un vacío normativo

preocupante, lo que significa que, los derechos a la imágen, la honra, la participación política y la privacidad han quedado debilitados (Piedra, 2024).

En el contexto descrito, el peligro es potencialmente grave por el simple hecho de que, en el entorno digital contemporáneo, ya no es necesario ser un experto o tener conocimientos y habilidades especializados para crear contenido falso hiperrealista. Cualquier persona puede encontrar y usar libremente las herramientas de IA para generar audios, videos e imágenes donde se simulan gestos, discursos y situaciones que nunca ocurrieron.

Trasladando lo antes mencionado al contexto de contiendas electorales, está la capacidad técnica puede ser utilizada para crear y difundir videos que buscan desprestigiar a ciertas candidaturas, atribuirles vínculos con el crimen organizado o simular sus expresiones en situaciones comprometedoras.

Este tipo de prácticas afectan al principio de transparencia democrática, consagrado en la Constitución de la República; en el Pacto Internacional de Derechos Civiles y Políticos, que garantiza el derecho a elecciones libres, basadas en una información veraz y en condiciones equitativas para todas las candidaturas.

Si bien, el artículo 500 del COIP (Código Orgánico Integral Penal [COIP], 2014) ya reconoce que el contenido digital puede ser un elemento probatorio y establece algunas normas sobre su recolección y análisis por un perito, la realidad es que no hay protocolos para determinar si la imágen generada por IA es auténtica, ni decisiones jurisprudenciales claras que guíen el proceso de valoración de esta evidencia, lo que hace que las víctimas sufran de una doble vulneración perpetuada, pues son vulneradas en su imágen y honra, y además, no logran una verificación de ilícito penal, de aquí que sea necesario adecuar el razonamiento jurídico a los entornos tecnológicos contemporáneos mediante la lógica de la

racionalidad comunicativa, la ponderación de derechos y el análisis de riesgos como señala R. Alexy.

Por su parte, iniciativas enérgicas como las Directrices Éticas sobre IA de la UNESCO o la reciente Ley de Inteligencia Artificial de la Unión Europea proponen clasificaciones por nivel de riesgo, una mayor transparencia algorítmica y diagnostican la creación de autoridades de supervisión tecnológica, temas que aún no han sido plenamente integrados al marco jurídico ecuatoriano (OCDE, 2019).

Violencia simbólica, género y manipulación política con IA

En el escenario de las tecnologías digitales y, más particularmente, de la inteligencia artificial, la violencia simbólica adquiere nuevas expresiones, como cuando se implementa en combinación con la manipulación política y estrategias de discriminación por género (Albaine, Paridad de género y violencia política. Los casos de Bolivia, Costa Rica y Ecuador, 2015).

En estos fenómenos, ha tomado protagonismo el uso de la IA durante los pasados procesos electorales en los cuales las candidatas mujeres, figuras jóvenes y disidentes del discurso hegemónico se convirtieron en objetivos de la agresión virtual algorítmicamente construido para degradar su imágen pública, cuestionar su autoridad y frenar su capacidad y derecho de agencia en el espacio político (Pérez & Izquierdo, 2024).

Un ejemplo que puede acreditar lo antes mencionado es el de la candidata presidencial Luisa González, en tanto, fue atacada con la difusión masiva de imágenes sexualidas generadas mediante IA para desprestigiar su campaña política y ser objeto de burlas (Deepfake).

Estos ataques cyberneticos se inscriben en una lógica estructural de violencia política de género, la que, en los entornos online, se repite a través de videos falsos, memes denigrantes e insultantes, hasta bots automatizados que hacen viral la misoginia; deepfakes,

conscientemente diseñados para erosionar la percepción pública de liderazgo (Vásquez, 2022).

Desde la perspectiva del ordenamiento jurídico ecuatoriano, ciertas conductas derivadas del uso malicioso de tecnologías digitales, podrían enmarcarse en principio, en figuras como la violencia contra la mujer o miembros del núcleo familiar y el hostigamiento digital previstos en el COIP. Sin embargo, la dificultad probatoria derivada de la falta de regulación específica de la violencia simbólica, y la falta de tipificación penal del uso de IA con fines de violencia deja vacíos de normativa claramente identificables y por ende, reduce la capacidad del Estado para responder de forma adecuada a agresiones que afectan la integridad de un proceso democrático.

La problemática demuestra, además, que la violencia simbólica mediada por tecnologías no se circunscribe al ámbito político: constituye una forma de agresión digital transversal cuyos efectos recaen con mayor intensidad en mujeres, niñas y adolescentes. Por ello, resulta incompatible con los principios de igualdad, dignidad y no discriminación reconocidos por la Constitución y los instrumentos internacionales de derechos humanos.

Ley de Inteligencia Artificial de la Unión Europea

La Unión Europea presenta avances significativos en materia jurídica que regula el uso de la IA y sus fines tecnológicos. La creación de la Ley de Inteligencia Artificial (Diario Oficial (DO) de la Unión Europea el 12 de julio de 2024); tiene como objetivo adaptar las nuevas tecnologías en el marco del respeto a los derechos universales. En concreto, el Capítulo II establece las prácticas prohibidas ante los potenciales usos de la IA, pues al ser sistemas generativos se autoalimentan a una escala global; entre ellas, «técnicas manipuladoras o engañosas, con el objetivo o el efecto de distorsionar sustancialmente el comportamiento de una persona o un grupo de personas, menoscabando apreciablemente su capacidad para tomar una decisión informada».

En tal sentido, el vertiginoso desarrollo de la inteligencia artificial en los ambientes digitales ha sacudido las bases sobre las cuales descansan los Derecho Penal, el Derecho Procesal y el Derecho a la imágen, evidenciando la necesidad de una redefinición de los referentes normativos en el ámbito del surgente desafío algorítmico. Tal es la postura de autores como Víctor Bazán, quien plantea que los sistemas normativos de matriz positivista resultan insuficientes para enfrentar las realidades fragmentarias y desarrolladas en la virtualidad de los delitos digitales, en donde el peregrinar criminal no puede ser imputado bajo las formas conocidas.

La idea de un autor material directo de la comisión del delito, causada por la condición IA, genera deducciones dogmáticas muy confusas para el sistema penal ecuatoriano, al no poder probar quién es el autor y no haber evidencia física o electrónica incriminatoria que invocar. Además, como se mencionó anteriormente, no se aplica la noción tradicional del dolo y, cuando la parte de la antijuridicidad no puede probarse, solo confirma este hecho.

La imposibilidad o dificultad probatoria que este contexto plantea desde una perspectiva procesal, constituye un serio obstáculo para la aplicación del principio de verdad procesal. Tal como señala Aulis Aarnio, la argumentación jurídica en ambientes digitales requiere herramientas epistémicas novedosas con capacidad de reconstruir cadenas de custodia en el ámbito de lo virtual, algo que el COIP aborda tangencialmente.

Desde mediados del siglo XX, las máquinas, los ordena-dores y los programas de Inteligencia Artificial han participado en distintos procesos creativos hasta convertirse en verdaderos «artistas robóticos» (Guadamuz, 2017). Las máquinas o los programas de IA eran un mero instrumento del ente pensante, sin ser realmente participes del proceso, hoy en día la realidad es otra, el avance tecnológico ha obligado a la sociedad a replantearse el tipo de trato que debe dársele a estos programas, así como su regulación y protección de derechos de

autor. De esta forma, esta revolución tecnológica destaca por la aparición de programas y softwares capaces de crear por sí solos y con completa autonomía obras de calidad artística. (Doval Escriva de Romaní, 2020)

Sin embargo, como se ha expuestos anteriormente, la ausencia de regulación a nivel nacional y mundial podría generar muchos problemas. En el caso que nos ocupa, la falta de autoría humana directa sobre los contenidos producidos por la IA impide la protección bajo el régimen convencional. La UNESCO indica que si no hay intervención creativa del ser humano, el producto está en un estado legal de limbo. Este estado embellece la falta de soluciones jurídicas a las víctimas, debido a que no pueden demandar o denunciar a quienes les han ocasionado daños morales o indirectos; no existe un propietario formal de la obra o una cara sobre quien imputar la responsabilidad delictual.

En China, por ejemplo, que los programas de Inteligencia Artificial creen de manera autónoma y exclusiva obras protegidas por derechos de autor, es ya una realidad. Ante ello, los expertos han empezado a visualizar en cada uno de los usos de la inteligencia artificial cuáles son los límites o de qué manera deben abordarse para garantizar que se mantiene la protección del ser humano (Rodríguez, 2020).

Propuesta

En razón de lo expuesto en los párrafos que anteceden, ante la problemática del uso con fines doloso de las tecnologías generativas, y su producto final, los deepfakes y fake news, aprovechados para la manipulación política, violencia digital, o intromisión a los derechos personalísimos, resulta necesario que nuestro ordenamiento jurídico ecuatoriano sea objeto de reformas que hagan frente a la impunidad de estas conductas, a través de una tipificación autónoma de la manipulación digital, falsificación, ambas generadas por inteligencia artificial.

Por lo que se propone la incorporación de un nuevo tipo penal autónomo en el Título IV del COIP, que regule los delitos informáticos, específicamente como nuevo conjunto de artículos derivado del 234 como se señala a continuación.

"Art. 234.5.- Falsificación digital mediante sistemas de inteligencia artificial o tecnologías similares:

La persona que, utilizando sistemas de inteligencia artificial o tecnologías similares, cree, elabore, genere, manipule, modifique, altere, reproduzca o difunda contenido audiovisual (verbos rectores), sonoro o gráfico, que reproduzca, imite o simule la imágen, voz, comportamiento o expresión de un tercero sin su consentimiento, con la finalidad de: a) Falsear la verdad, b) Afectar su reputación, c) Causar daño político, económico, psicológico o moral, d) O influir en procesos electorales, judiciales o administrativos; será sancionada con pena privativa de libertad de tres a cinco años, y una multa de diez salarios básicos unificados del trabajador en general, sin perjuicio de las sanciones por delitos concurrentes.

Si el contenido producido involucra a personas menores de edad, personas con discapacidad, figuras de autoridad, candidatas o candidatos a cargos de elección popular, o se utiliza para cometer actos de violencia simbólica o de género, la pena será de cinco a siete años."

Quien a sabiendas que la información es producto de la creación de sistemas de inteligencia artificial, difunda, comparta, o transmita por cualquier medio o plataforma digital o red social, contenido falso manipulado por sistemas de inteligencia artificial con la finalidad de causar daño, se le aplicará un tercio de la pena y una multa de tres a ocho salarios básicos unificados del trabajador en general.

Tabla 1

Propuestas normativas y procesales frente a la manipulación con sistemas de IA en Ecuador

Artículo	Conducta sancionada	Finalidad o daño	Sanción básica	Agravantes	Sanción agravada
234.5	Falsificación digital mediante IA	Desinformar, afectar reputación, causar daño político, económico, psicológico o influir en procesos	3–5 años prisión + multa 10 SBU	Menores, discapacidad, autoridades, candidatos, violencia simbólica o de género	5–7 años prisión
234.5 (difusión)	Difundir contenido falso manipulado por IA a sabiendas	Causar daño	⅓ de la pena + multa 3–8 SBU	—	—
234.6	Suplantación de identidad mediante IA	Obtener beneficio ilícito o causar perjuicio	4–6 años prisión + multa 5–10 SBU	Extorsión, fraude, daño moral o psicológico	6–8 años prisión
234.7	Manipulación de contenido digital con fines electorales ilícitos	Influir ilícitamente en procesos electorales	5–7 años prisión + multa 6–12 SBU	Afecta candidatos, partidos o procesos en curso	7–9 años prisión
234.8	Creación y difusión de deepfakes para violencia simbólica o de género	Ejercer violencia simbólica o de género	6–8 años prisión + multa 7–15 SBU	Víctima menor, discapacidad, autoridad, candidata/o	8–10 años prisión
Disposición Transitoria Única	Vigencia	Aplicable desde su publicación en Registro Oficial a casos en trámite o futuros	—	—	—

Nota: (Bryan Aníbal, 2025)

La propuesta normativa es pertinente y necesaria en tanto aborda una realidad tecnológica y social carente de suficiente respuesta punitiva en el marco de la legalidad ecuatoriana vigente. La creación de tipos penales específicos para casos de falsificación digital, suplantación de identidad, manipulación electoral, es decir, conductas atribuibles al uso de la IA con fines dolosos en general, es idónea para cerrar la evidente laguna legal y reconocer los daños reales ocasionados por estos actos.

Asimismo, resulta compatible con los principios constitucionales que garantizan los derechos personalísimos, así como la equidad en el ámbito de la competencia electoral y tutela judicial efectiva, al proporcionar una herramienta más clara de investigación, imputación y sanción. Esta medida contribuye a la disuasión de potenciales infractores y al

recobro de la confianza ciudadana en los procesos democráticos y judiciales, en fiel cumplimiento a la seguridad jurídica.

En cuanto a la viabilidad, la propuesta es técnicamente factible, siempre que se acompañe de medidas institucionales y técnicas. Por ejemplo, será necesario invertir en educación, fiscalía, judicatura; y, fortalecer la pericia con respecto a la manipulación de la evidencia digital y el proceso de la inteligencia artificial, para garantizar la eficacia de los tipos de delitos cibernéticos. También será necesario establecer unidades especializadas de cibercrímen con los recursos necesarios, para avanzar hacia la protección efectiva de los derechos en el ámbito digital.

Discusión

Los hallazgos de este estudio confirman que el uso doloso de sistemas de inteligencia artificial —en particular, las deepfakes audiovisuales— erosiona aceleradamente bienes jurídicos personalísimos (honra, imágen e identidad digital) y tensiona categorías clásicas del Derecho penal y procesal penal (autoría, dolo, nexo causal y prueba), especialmente en contextos electorales (Arcos-Chaparro & Epia-Silva, 2024). La hiperrealidad de los contenidos sintéticos amplifica la incertidumbre epistémica del público, deteriora la confianza informativa y potencia la eficacia de la desinformación política. Estos efectos, observados también en el escenario ecuatoriano descrito en el manuscrito, refuerzan la necesidad de una respuesta normativa específica y tecnoprocesalmente informada (Barzola-Plúas, 2022).

En primer término, la amenaza no se limita a la verosimilitud de la manipulación, sino a su escalabilidad, bajo coste y opacidad algorítmica, factores que desdibujan el iter criminis y facilitan la «autonomía operativa» de la agresión digital. Ello explica la dificultad práctica —también constatada en este trabajo— para identificar al autor material o intelectual y para

preservar una cadena de custodia robusta cuando el contenido se replica en redes distribuidas y plataformas efímeras. La forensia multimedia, además, enfrenta límites sustantivos: los detectores automatizados son sensibles a cambios de dominio, compresión y ataques adversariales, por lo que su rendimiento decae fuera del entorno de entrenamiento; en consecuencia, no constituyen por sí solos un estándar probatorio irrefutable (Barahona-Martínez et al., 2024). Esta convergencia entre retos tecnológicos y déficits procesales robustece la tesis central del artículo: el marco vigente es insuficiente para tutelar eficazmente los derechos afectados y para disuadir el uso malicioso de IA (Bonilla-Morejón, 2023).

En segundo lugar, desde una perspectiva de epistemología jurídica, la «desancladura» de lo audiovisual como backstop epistémico —tradicionalmente clave para corroborar testimonios y reconstruir hechos— multiplica el valor corrosivo de las deepfakes en procesos electorales y penales. Si las grabaciones dejan de ofrecer un suelo común de veridicción, los incentivos para el negacionismo estratégico se incrementan y la litigación sobre autenticidad desplaza la discusión de fondo. Esta deriva es coherente con los casos mediáticos reseñados en el estudio y con la constatación de que los datos biométricos (rostro y voz) circulan y se reutilizan sin consentimiento, en entornos regulatorios que no habían previsto la síntesis generativa a escala (Núñez-Ribadeneyra, 2023).

En tercer lugar, la comparación con la experiencia internacional sugiere que la respuesta penal no puede agotarse en «reencuadrar» figuras tradicionales —como la falsificación informática o el hostigamiento digital—. El vector delictivo de las deepfakes combina: (i) apropiación y manipulación de datos biométricos; (ii) fabricación de evidencia o suplantación performativa; (iii) daño reputacional y afectación de procesos electorales; y (iv) ocultamiento de autoría mediante infraestructuras distribuidas. Por ende, resulta persuasiva la propuesta de configurar un tipo penal autónomo de «manipulación digital dolosa mediante

IA», con elementos objetivos y subjetivos diferenciados: conductas nucleares de generación, difusión masiva y/o puesta a disposición de contenido sintético no consentido con ánimo de causar perjuicio; dolo específico; y agravantes por contexto electoral, minoridad o violencia sexual. Ello debe acompañarse de reglas procesales ad hoc para la preservación y acreditación de autenticidad e integridad digital (Samaniego-Quiguiri & Bonilla-Morejón, 2024).

Complementariamente, la evidencia sugiere líneas de compliance y prevención con relevancia penal y para la reparación integral: (a) obligaciones de due diligence algorítmica y trazabilidad (provenance y «marcas de agua» robustas) en proveedores de modelos y plataformas; (b) deberes reforzados de respuesta y retiro expedito ante reportes verificados, en especial durante periodos electorales; y (c) estandarización pericial —protocolos de adquisición, hashing, conservación y reporte probabilístico de autenticidad— para reducir litigios sobre fiabilidad técnica y trasladar la controversia al plano del dolo y la lesividad. Aunque estas medidas no sustituyen el tipo penal, operan como ex ante preventivo y ex post facilitador de la prueba (Barzola-Plúas et al., 2023).

Finalmente, en coherencia con los resultados reportados, este trabajo presenta implicaciones político-criminales nítidas: (i) incorporar cláusulas de protección reforzada en procesos electorales, dada la mayor capacidad de daño cívico de las deepfakes en dichas fases; (ii) articular un título o capítulo específico de delitos informáticos que reconozca la singularidad etiológica y probatoria de la IA generativa; y (iii) promover la formación interdisciplinaria de fiscales, jueces y peritos en forensia multimedia y epistemología de la prueba digital, para evitar estándares probatorios inalcanzables o asimetrías técnicas que deriven en impunidad. Sin estos ajustes, la brecha entre daño real y sanción eficaz previsiblemente se ampliará (Mendoza-Armijos et al., 2023).

Conclusión

En el presente trabajo de investigación se ha logrado determinar que el avance significativo de la inteligencia artificial ha generado un escenario en el que; lejos de la crítica ideológica o partidista, las modalidades descritas se sustentan en prácticas de falsificación digital, desinformación, manipulación, violencia simbólica, entre otras, que afectan no solo a la libertad de expresión y de reunión, sino también a derechos como la imágen, la honra y la participación en un plano de igualdad, tal como lo demuestran los casos documentados en los procesos presidenciales de 2021 y 2023, contra figuras públicas y ciudadanos comunes.

El derecho a la imágen, a pesar de encontrarse contemplado en la Constitución ecuatoriana, no cuenta con una regulación especializada sobre los entornos digitales e hiperconectados, lo cual permite la producción y circulación masiva de los contenidos alterados sin el respectivo consentimiento. Este vaivén legal deja en estado de indefensión a las víctimas, en especial en los escenarios de violencia de género, política o vicaria, donde estos contenidos generados por la IA se transforman en un arma de agresión de alta replicabilidad y baja trazabilidad.

En cuanto al delito, la comisión a través de sistemas de IA también implica un cambio de paradigma con respecto al clásico, mientras que la configuración del iter criminis, la imputabilidad del hecho y la inexistencia de autoría material directa tienen a las acciones como «fantasmas», de allí la dificultad en el alcance de las herramientas normativas y técnicas que permitan la incorporación de mecanismos en el entorno digital generativo subsiguiente.

La ausencia de mecanismos penales y procesales específicos, sumada a la dificultad para identificar autores y autenticar técnicamente material producido por sistemas generativos, evidencia vacíos que comprometen la tutela judicial efectiva y el debido proceso. Estos déficits normativos afectan de manera desproporcionada a grupos históricamente

vulnerables, especialmente mujeres, niñas y adolescentes, al mismo tiempo, pueden proyectarse hacia el ámbito político, donde contribuyen a reproducir formas de violencia simbólica y digital.

Por otra parte, el tratamiento jurídico de la IA no puede dejar de lado una perspectiva del Derecho de la Propiedad Intelectual, dado que la no autoría humana de los contenidos creados genera graves dificultades, sobre todo, la autoría y titularidad de los derechos de propiedad intelectual y la imputación de responsabilidad en los casos de daños potenciales. Por lo que no solo la reforma del Código Orgánico Integral Penal resulta necesaria, sino que también se recomienda que el Código Orgánico de la Economía Social del Conocimiento, Creatividad e Innovación (Código Ingenios) también sea reformado, considerando el ejemplo de China antes expuesto.

Referencias bibliográficas

Albaine. (2015). *Paridad de género y violencia política. Los casos de Bolivia, Costa Rica y Ecuador*. Integridad y equidad electoral en América Latina.

Albaine. (2021). *Violencia política contra las mujeres por motivos de género en América Latina: Estrategias legales y el rol de los organismos electorales*.

Alonso, M., & Sánchez, H. M. (2024). Inteligencia artificial en la verificación de la información política. Herramientas y tipología. *Más Poder Local, 1*(56), 27-45. https://doi.org/10.56151/maspoderlocal.215

Alvarez, H. (2023). La Inteligencia Artificial como Catalizador en la Enseñanza de la Historia: Retos y Posibilidades Pedagógicas. *Revista Tecnológica-Educativa Docentes 2.0, 16*(2). https://doi.org/10.37843/rted.v16i2.426

Arcos-Chaparro, I. A., & Epia-Silva, M. A. (2024). La transverzalización del debido proceso en las relaciones laborales particulares. *Journal of Economic and Social Science Research*, *4*(2), 17–43. https://doi.org/10.55813/gaea/jessr/v4/n2/100

Arias, F. (2006). *El Proyecto de Investigación: Introducción a la metodología científica.* Episteme.

Asamblea Nacional. (2018). *Ley Orgánica integral para la prevención y erradicación de la VIolencia de Género contra las mujeres.* https://oig.cepal.org/sites/default/files/2018_ecu_leyintegralprevencionerradicacionviolenciagenero.pdf

Baños, G. (2024). *El sueño de la Inteligencia Artificial: El proyecto de construir máquinas*

pensantes: una historia de la IA. Shackleton Books.

Barahona-Martinez, G. E., Barzola-Plúas, Y. G., & Peñafiel-Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, *4*(3), 46–64. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. *Revista Científica Zambos*, *1*(1), 86-101. https://doi.org/10.69484/rcz/v1/n1/23

Barzola-Plúas, Y. G., Samaniego-Quiguiri, D. P., Núñez-Ribadeneyra, R. A., & Bonilla-Morejón, D. M. (2023). Protección de datos personales en la era de la computación cuántica y sus desafíos legales. *Revista Científica Ciencia Y Método, 1*(3), 45-57. https://doi.org/10.55813/gaea/rcym/v1/n3/19

Bonilla-Morejón, D. M. (2023). Derecho Penal y Políticas de Seguridad en Ecuador: Análisis de la Eficacia. *Revista Científica Zambos*, *2*(3), 59-74. https://doi.org/10.69484/rcz/v2/n3/50

Borja, C. (2023). Utilización y modificación de obras protegidas por el derecho de autor en fotografías publicadas en el entorno digital. *USFQ Law Review, 10*(1), 11.

Borja, V. (2024). Reflexiones Jurídico-Éticas sobre Genética, Inteligencia Artificial y el Futuro de los Derechos Humanos. *Eirene Estudios de Paz y Conflictos, 7*(12), 111-138.

Código Orgánico de la Economía Social de los conocimientos, creatividad e innovación. (9 de 12 de 2016). Registro Oficial Suplemento 899: https://site.inpc.gob.ec/pdfs/lotaip2020/Codigo%20Organico%20de%20la%20%20Economia%20Social%20de%20los%20Conocimientos.pdf

Código Orgánico General de Procesos, COGEP. (2015). Quito-Ecuador: Disposición reformatoria cuarta de la Ley No. 1. Disposición Reformatoria Cuarta de Ley No. 1, publicada en Registro Oficial Suplemento 452 de 14 de Mayo del 2021: https://www.lexis.com.ec/biblioteca/cogep

Código Orgánico Integral Penal [COIP]. (2014). Quito-Ecuador: Ley No. 1. Clave: 15631. Registro Oficial Suplemento 180.

Constitución de la República [CRE]. (2008). Montecristi-Ecuador: Registro Oficial No. 449. https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf

Crawford, K. (2018). *Atlas de inteligencia artificial: Poder, política y costos planetarios.* Tezontle.

Devis, A. (2025). *La desinformación en la sociedad digital: aspectos criminológicos, dogmáticos y de política criminal.* Universidad de Valencia RODERIC.

Díaz, F., & Osorio, M. (2023). Una mirada de Inteligencia Artificial, desde el impacto global a los efectos locales. *Question , 3*(76), 18. https://doi.org/10.24215/16696581e862

Doval Escriva de Romaní, A. (2020). Inteligencia Artificial y Propiedad Intelectua: ¿Puede un sistema de Inteligencia Artificial crear obras protegidas por Derechos de Autor? *Universidad Pontifica Comillas*.

Feria, A. (2022). El derecho al entorno digital: una aproximación. *Revista española de derecho militar, 118*, 167-215.

Galarza, L. (1998). *Metodología de la investigación Luis Enrique Galarza.* Vértice studio.

García, J. (24 de noviembre de 2023). *América Latina ante la inteligencia artificial: mapeo de iniciativas regulatorias en la región*. https://www.derechosdigitales.org/22881/america-latina-ante-la-inteligencia-artificial-mapeo-de-iniciativas-regulatorias-en-la-region/

Gargallo, S., & Cesteros, P. (2022). Metodología de la investigación en la enseñanza-aprendizaje del español como segunda lengua (L2)/lengua extranjera (LE). *Revista didáctica de español y lengua extranjera*(34), 392.: https://www.academia.edu/80258918/METODOLOG%C3%8DA_DE_LA_INVESTIGACI%C3%93N_EN_LA_ENSE%C3%91ANZA_APRENDIZAJE_DEL_ESPA%C3%91OL_COMO_SEGUNDA_LENGUA_L2_LENGUA_EXTRANJERA_LE

Garriga, A. (2024). Los derechos ante los sistemas biométricos que incorporan Inteligencia Artificial . *Monográfico "Derechos e Inteligencia Artificial"* (51), 117-149. https://doi.org/10.20318/dyl.2024.8585

Gilas. (2020). *Violencia política en razón de género y armonización legislativa multinivel en México*. Derecho Electoral.

Giletta, M., Mercaú, Orden, & Villareal. (2020). Inteligencia Artificial: definiciones en disputa. *Sociales Investiga* (9), 20-33. https://socialesinvestiga.unvm.edu.ar/ojs/index.php/socialesinvestiga/article/view/320

Guadamuz, A. (2017). *La Inteligencia Artificial y el derecho de autor.* Revista de la OMPI (5) 1-12.

Gutiérrez, C., & Abeliuk, A. (2022). Historia y evolución de la inteligencia artificial . *Inteligencia artificial* , 8.

La Tercera . (2022). *Colektia, que utiliza la inteligencia artificial para facilitar el trabajo de la cobranza, tuvo un crecimiento explosivo de un 400% durante 2020.* e https://www.latercera.com/piensa-digital/noticia/fintech-cobranza-digital/1017447/

Malo, A., & Lozano, R. (2024). *La injerencia de la inteligencia artificial en la violación a la privacidad en las redes sociales [Tesis, Universidad del Azuay]*. https://dspace.uazuay.edu.ec/handle/datos/14857

Medina, C. (2025). Robótica, Inteligencia Artificial y Derecho: Nuevas Dimensiones Jurídicas en el Siglo XXI. *Ciencia Latina, 9*(1), 9488-9513. https://doi.org/10.37811/cl_rcm.v9i1.16574

Mendoza, O. (2022). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS, 15*(48). https://doi.org/10.35487/rius.v15i48.2021.743

Mendoza-Armijos, H. E., Camacho-Medina, B. M., & García-Segarra, H. G. (2023). Análisis de la justicia restaurativa como alternativa al sistema penal tradicional en América Latina. *Revista Científica Ciencia Y Método, 1*(3), 58-69. https://doi.org/10.55813/gaea/rcym/v1/n3/20

Ministerio de Telecomunicación y de la Sociedad de la Información. (2021). *Diagnóstico*

sobre la Inteligencia Artificial en el Ecuador. HITO 20: https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2022/11/Proyecto-diagnostico-inteligencia-artificial-IA-en-Ecuador-Documento-final-JC-JO-MS-002.pdf

Mondria, T. (2023). Innovación MedIÁtica: aplicaciones de la inteligencia artificial en el periodismo en España. *Visual Media, 17*(1), 41-60. https://doi.org/10.56418/txt.17.1.2023.3

Montes, D. (2024). *La vulneración del derecho a la intimidad ya la privacidad en el entorno digital en el Perú.* ESAN. https://repositorio.esan.edu.pe/items/14f003ee-7233-43e8-8d3c-3eae2d966c1a

Muñoz, A. (2024). Los sistemas automatizados de reconocimiento de emociones en el trabajo en el reglamento europeo de inteligencia artificial. *LABOS Revista de Derecho del trabajo y protección social , 5*. https://doi.org/10.20318/labos.2024.9033

Núñez-Ribadeneyra, R. A. (2023). Derechos Humanos y Justicia Social en el Contexto Ecuatoriano. *Revista Científica Zambos*, *2*(3), 42-58. https://doi.org/10.69484/rcz/v2/n3/49

OCDE . (13 de agosto de 2019). *Los principios de Inteligencia Artificial de la OCDE*. https://datos.gob.es/es/blog/los-principios-de-inteligencia-artificial-de-la-ocde

Ojeda, K. (2024). *La inteligencia artificial, un análisis desde el derecho comparado con España y Colombia.* [Tesis]: Universidad de los Andes: https://dspace.uniandes.edu.ec/bitstream/123456789/18532/1/USD-DER-EAC-021-2024.pdf

ONU Mujeres . (2023). *En Ecuador se ha dado una sede de casos de violencia política contra las mujeres la cual se manifiesta de distintas formas como lo son la violencia física violencia por medios digitales y violencia dentro de los partidos políticos en las que las mujeres f.* https://ecuador.unwomen.org/es/que-hacemos/liderazgo-y-participacion-politica/violencia-politica#:~:text=De%20acuerdo%20con%20el%3A%20%E2%80%9CEstudio%20sobre%20violencia%20pol%C3%ADtica,mujeres%20est%C3%A1n%20m%C3%A1s%20expuesta%20a%20la%20violencia%20po

Organización de las Naciones Unidas. (10 de julio de 2024). *¿Puede la Inteligencia Artificial influenciar los procesos electorales?* Organización de las Naciones Unidas: https://unric.org/es/peligros-y-beneficios-de-la-inteligencia-artificial-en-procesos-electorales/

Peña, N. (2021). Big data e inteligencia artificial: una aproximación a los desafíos éticos y jurídicos de su implementación en las administraciones tributaria. *Ius et Scientia, 7*(1), 62-84.

Peña-Terán. (2023). *Mecanismos procesales para el eficaz tratamiento de las infracciones electorales de violencia política de género en Ecuador 2020–2022*. UCE.

Pérez, C., & Izquierdo, Y. (2024). Violencia política contra las mujeres. *Emerging Trends in Education, 2*(4).

Pérez, P. (2023). Cuestiones éticas sobre la implantación de la inteligencia artificial en la administración pública. *Revista Canaria de Administración Pública*, 243-282.

Piedra, J. (2024). Democracias generativas: inteligencia artificial y manipulación en el siglo XXI. *Trajectoires Humaines Transcontinentales*(1), 5. https://doi.org/10.25965/trahs.6334

Priego, V. (2022). Los derechos de las personas menores de edad en entornos digitales: oportunidades, riesgos y protección. *Protección jurídica de las personas menores de edad: Un estudio multidisciplinar*, 119-180. https://www.torrossa.com/en/resources/an/5494797

Pulido, I. (2023). El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes. *IUS ET SCIENTIA, 9*(2), 157-180.

Revelo, R. (17 de junio de 2024). "Con la Inteligencia Artificial, hay mucha información expuesta", alerta experta de ciberseguridad. *Primicias*. https://www.primicias.ec/noticias/entretenimiento/tecnologia/inteligencia-artificial-datos-proteccion-ciberseguridad-ataques/

Revista Vistazo . (23 de octubre de 2023). *Alumnos de un colegio de Quito usaron inteligencia artificial para crear videos sexuales con los rostros de sus compañeras* . https://www.vistazo.com/actualidad/nacional/alumnos-de-un-colegio-de-quito-usaron-inteligencia-artificial-para-crear-videos-sexuales-con-los-rostros-de-sus-companeras-ME6107394

Rodríguez, Á., Rodríguez, F., Collaguazo, D., & Rodríguez, J. (2024). Diferencias y Aplicaciones de Big Data, Inteligencia Artificial, Machine Learning y Deep Learning . *Revista Científica POCAIP, 10*(3). https://doi.org/10.23857/dc.v10i3.3966

Rouhiainen, L. (2018). *Inteligencia artificial.* Alienta Editorial.

Samaniego-Quiguiri, D. P., & Bonilla-Morejón, D. M. . (2024). Análisis de la Evolución del Derecho Constitucional en Ecuador: Implicaciones para el Desarrollo Democrático. Revista Científica Zambos, 3(3), 1-14. https://doi.org/10.69484/rcz/v3/n3/53

Sampieri, R. H. (2014). *Metodología de la investigación.* McGraw-Hill.

Sanz, A. (2025). *El Reglamento Europeo de Inteligencia Artificial: análisis jurídico del uso de la biometría.* [PCEO de Administración]. Universidad de Oviedo: https://digibuo.uniovi.es/dspace/handle/10651/77211

Secretaría de Marina. (2021). *Metodología de la Investigación.* SEMAR- Universidad Naval. https://www.gob.mx/cms/uploads/attachment/file/133491/METODOLOGIA_DE_INVESTIGACION.pdf

Solar, J. (2021). *Retos de la deontología de la abogacía en la era de la inteligencia artificial jurídica.* Dykinson.

Tarrillo, L. (2024). *Importancia del Iter Criminis en la tipificación del delito.* UPCI.

Trujillo, C. (2024). El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial . *InDret*, 1-40.

Ulloa, M. (1 de octubre de 2024). *Avances en la regulación de la Inteligencia Artificial en América Latina*. Observatorio de Riesgos catastróficos Globales: https://orcg.info/articulos/avances-en-la-regulacin-de-la-inteligencia-artificial-en-amrica-latina

UNESCO. (30 de agosto de 2023). *Recomendación sobre la ética de la inteligencia artificial*. https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

Varona, G. (2024). Evidenciar la violencia estatal y corporativa hacia los ecosistemas a través de la arquitectura forense digital. *Boletín Criminológico, 30*(30).

Vásquez, R. (28 de septiembre de 2023). Estos son los riesgos de usar la inteligencia artificial en los procesos electorales. *Artículo web* , 2. México , México. https://forbes.com.mx/los-riesgos-de-la-inteligencia-artificial-en-los-procesos-electorales/

Vásquez. (2022). *Políticas públicas contra la violencia de género en el Ecuador*. RECIMUNDO: https://recimundo.com/index.php/es/article/view/1581