Verdad y Derecho
Revista Arbitrada de Ciencias Jurídicas y Sociales
Vol. 4(Especial), 325-343, 2025
https://doi.org/10.62574/r083dh53

Evidencias Deepfake en sistema penal ecuatoriano: reconocimiento, autenticidad y aceptación probatoria en juicios

Deepfake evidence in the Ecuadorian criminal justice system: recognition, authenticity, and admissibility in trials

Brandon Paul Adriano-Caiza
ur.brandonac62@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Chimborazo, Ecuador
https://orcid.org/0000-0002-5510-6019

Viviana Del Rocío Marfetan-Marfetan
ur.vivianamm31@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Chimborazo, Ecuador
https://orcid.org/0009-0008-1144-0200

Mesías Elías Machado-Maliza
luisacm08@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Riobamba, Chimborazo, Ecuador
https://orcid.org/0000-0002-5815-1093

RESUMEN

Se tiene por objetivo determinar los instrumentos legales y procesales que, apoyados en criminalística, sirven para la detección de elementos generados con tecnología deepfake en el procedimiento penal ecuatoriano. Investigación cualitativa, utilizando análisis documental y revisión bibliográfica. Se examinó normativa vigente, capacidades institucionales del Servicio Nacional de Medicina Legal y Ciencias Forenses, y literatura especializada en tecnologías de detección. El COIP carece de regulación específica sobre evidencias generadas con inteligencia artificial. El SNMLCF posee pericias en ingeniería informática forense, análisis de voz e identidad morfológica, pero sin especialización específica en detección deepfake. La cadena de custodia digital (artículos 456-457 COIP) constituye el principal mecanismo de verificación de autenticidad. Existe brecha significativa entre el avance tecnológico deepfake y la capacidad institucional ecuatoriana de detección. Se requiere actualización normativa específica, fortalecimiento de capacidades técnicas del SNMLCF, cooperación interinstitucional e internacional para garantizar tutela judicial efectiva.
Descriptores: tecnología, evidencia, derecho penal. (Fuente: Tesauro UNESCO).

ABSTRACT

The objective is to determine the legal and procedural instruments that, supported by criminalistics, serve to detect elements generated with deepfake technology in Ecuadorian criminal proceedings. Qualitative research, using documentary analysis and bibliographic review. Current regulations, institutional capacities of the National Service of Legal Medicine and Forensic Sciences, and specialised literature on detection technologies were examined. The COIP lacks specific regulations on evidence generated with artificial intelligence. The SNMLCF has expertise in computer forensics, voice analysis and morphological identity, but no specific specialisation in deepfake detection. The digital chain of custody (Articles 456-457 COIP) is the main mechanism for verifying authenticity. There is a significant gap between advances in deepfake technology and Ecuador's institutional capacity for detection. Specific regulatory updates, strengthening of the SNMLCF's technical capacities, and inter-institutional and international cooperation are required to ensure effective judicial protection.
Descriptors: technology, evidence, criminal law. (Source: UNESCO Thesaurus).

Recibido: 05/07/2025. Revisado: 19/07/2025. Aprobado: 27/07/2025. Publicado: 08/08/2025.
Sección artículos de investigación

INTRODUCCIÓN

La inteligencia artificial supone una auténtica revolución en numerosos campos de la sociedad; el Derecho no es una excepción, siendo que en el decurso de un procedimiento penal esta revolución también está presente. Ahora, dentro del ámbito procesal y enfocado el estudio en la práctica probatoria surge grandes interrogantes respecto a la admisibilidad y validez de la prueba, pues cada vez es más común generar o manipular a través de la inteligencia artificial no solo documentos, sino también imágenes, vídeos, audios, etc., que complejizan el debate probatorio y a su vez los bienes jurídicos protegidos, causando graves problemas legales y técnicos para el Derecho Procesal Penal.

Las denominadas *deepfakes* o también llamadas falsedades profundas, son aquellos elementos tales como vídeos, audios o imágenes que han sido generadas o manipuladas con software de inteligencia artificial y que tienen la apariencia de originales. Este tipo de falsedades son más comunes en los últimos años, debido a la revolución digital que ha supuesto la inteligencia artificial en la vida cotidiana.

Desde el año 2023 empezó a ser más recurrente el acceso a todo el público de estas herramientas, a través de aplicaciones móviles y demás software existente, por lo tanto, a día de hoy es muy común encontrar en la web y en redes sociales cómo se puede alterar la voz de una persona para que se escuche como alguien completamente diferente, al igual que de forma lamentable se empezaron a generar vídeos de carácter sexual en los que se coloca el rostro de una persona distinta al del vídeo original, provocando serios conflictos de difícil resolución en el ámbito probatorio del proceso penal.

Los *deepfakes* son la punta del iceberg de lo que pasará con la imagen y cualquier otro soporte de contenidos en el universo digital y sobre todo, en la lógica de la construcción de discursos falsos y mal intencionados en la laberíntica trama de las prácticas de la posverdad. Son parte de una familia que empieza a ser numerosa,

dominada o acompañada por los adjetivos *deep* y *fake*: *fake news, cheapfakes, fake nudes, shallow fakes, deep learning, deep web, deepnude*, etc. (Bañuelos Capistrán, 2020).

Frente a todo ello el Código Orgánico Integral Penal (COIP) tiene un acercamiento nulo sobre el uso y validez de la prueba generada con inteligencia artificial, más aún cuando la inteligencia artificial ha tomado relevancia desde el 2019 y el COIP fue promulgado en el 2014. A ello hay que sumar que el COIP es muy genérico al regular la prueba en contenido digital, dejando de lado algún tipo de regulación sobre los riesgos a nivel legal y procesal que supone el uso de estas herramientas tecnológicas.

El artículo 453 del COIP determina que la finalidad de la prueba es llevar al convencimiento de los hechos y circunstancias materia de la infracción, que como conceptualización general está bien, sin embargo, el cómo hacerlo es lo que genera una gran incertidumbre, más cuando se trata de elementos digitales. Para ello, la norma adjetiva prevé que la prueba en contenido digital debe estar sometida a cadena de custodia para así garantizar su autenticidad. Además, se determinan algunos criterios de valoración de la prueba, indicando que se debe tener en cuenta la legalidad, autenticidad, cadena de custodia y grado de aceptación científica y técnica de los informes periciales.

Ahora, la falta de recursos estatales avanzados y actualizados, de personal especializado y, de una normativa específica sobre la tecnología *deepfake* y demás herramientas tecnológicas incipientes, actualmente acarrea un problema crítico que permita garantizar lo que pregona el Código Orgánico Integral Penal respecto a la verificación de autenticidad de la prueba digital, suponiendo un enorme reto para la garantía de la tutela judicial efectiva.

En virtud de aquello, el problema queda más que evidenciado, razón por la cual el presente trabajo tiene como objetivo determinar los instrumentos legales y procesales que, apoyados en la criminalística sirven para la detección de elementos

generados con tecnología *deepfake*, los cuales pueden ocasionar un perjuicio al procedimiento penal.

Por lo tanto, se tiene por objetivo determinar los instrumentos legales y procesales que, apoyados en criminalística, sirven para la detección de elementos generados con tecnología deepfake en el procedimiento penal ecuatoriano.

MÉTODO

El presente trabajo responde a una investigación con un enfoque cualitativo, de tipo no experimetal, con el uso de analisis documental bajo la recopilación bibliográfica del tema. En cuanto a los métodos utilizados se destaca el análisis deductivo.

El trabajo de investigación mantiene sus límites en la descripción del fenómeno a partir de la investigación bibliográfica, la comparación con otras investigaciones y el análisis crítico sobre el fenómeno actual que se encuentra en Ecuador sobre las *deepfakes* y el sistema procesal penal, a fin de determinar la situación nacional actual e identificar todas las virtudes o falencias existentes y, perfectibles de ser el caso.

El estudio de esta temática resulta de gran importancia, toda vez que a pesar de encontrarnos ya en esta cuarta revolución industrial, debido al avance tecnológico, Ecuador sigue manteniendo un puesto relegado en el desarrollo de tecnologías emergentes destinadas a la identificación de las *deepfakes;* cuestión que se traduce en un perjuicio cada vez más grande a las personas en contra de quien se utiliza esta tecnología. Además, de no contar con una gran cantidad de trabajos investigativos en torno a esta problemática que esté centrada en el Derecho Penal ecuatoriano.

Conceptualización de deepfake

La palabra *deepfake* es un anglicismo cada vez más utilizado y extendido a nivel global. Etimológicamente está compuesto de dos vocablos, por un lado, *deep,* el cual significa profundo y por otro lado *fake* que significa falso. Estos vocablos

dentro de las ciencias informáticas se usan para referirse al aprendizaje profundo que se genera a través de las tecnologías de la inteligencia artificial.

El desarrollo de la inteligencia artificial, entre otras cosas, se basa en las denominadas redes generativas antagónicas o por sus siglas en inglés GANs (Generative Adversarial Networks), la cual consiste en la confrontación de dos redes neuronales:

- La generativa: Dedicada a la creación de elementos gráficos, los cuales suelen ser erróneos.
- La discriminadora: Dedicada y entrenada a la identificación, la cual analiza lo producido por la red generativa y permite realizar ajustes más exactos a lo solicitado (Merino, 2019).

Después de ello, *fake* se usa para referirse a aquellos elementos generados o producidos por inteligencia artificial que son falsos, basados en representaciones sintéticas, generando de esta manera las falsedades profundas.

La tecnología *deepfake* se basa en algoritmos complejos y sofisticados, que, a pesar de serlo, el resultado se obtiene en cuestión de escasos minutos, aun sin necesidad de dar indicaciones profundas o extremadamente elaboradas, evidenciando de esta manera los pasos agigantados en los que se coloca respecto a las personas de pie. En definitiva, la tecnología avanza mucho más rápido de lo que imaginamos y cada vez se hace más difícil alcanzarla y más aún regularla normativamente de manera adecuada.

Rápidamente empezó a extenderse en otros ámbitos, como el político, artístico y últimamente se extiende al ámbito empresarial, científico, social y jurídico (Coaquira Flores, 2025).

Muchas personas consideran que las *deepfakes* son una evolución a las ya conocidas *fake news* o noticias falsas, las cuales generalmente son producidas por el accionar humano directo, donde de manera intencionada se crea y propaga información no contrastada y eminentemente falsa e incorrecta. La particularidad de

las *deepfakes* es que son creadas a partir del uso de la inteligencia artificial, entre las cuales encuentra:

- Deepfaces: **son Deepfakes que consisten en crear imágenes (ya sea en audio o vídeo) convincentes, aunque completamente falsas, desde cero.**
- **Deepvoices: destinadas a la suplantación de la voz de una persona en audio** (*Deepfakes*, s. f.).

Además de existir otros términos que van emergiendo, tales como las *fake news, cheapfakes, fake nudes, shallow fakes, deep learning, deep web, deepnude*, entre otros que van apareciendo paulatinamente.

Las *deepfakes* como medio para la comisión de infracciones penales

Bien es cierto que las *deepfakes* tienen como propósito la creación y difusión de información falsa, de hecho, los primeros usos indebidos se lo hicieron para la producción de material pornográfico, extendiéndose de forma extremadamente acelerada para:

- Propagar noticias falsas.
- Generar desinformación.
- Desacreditar a alguien:
- Cometer delitos relacionados con el honor, la imagen o el fraude.
- Influir en las votaciones o toma de decisiones o pensamiento grupal.
- Llevar a cabo venganzas.
- Manipular los mercados financieros.
- Desestabilizar las relaciones internacionales (*Deepfakes*, s. f.).

Existe hasta la actualidad casos relevantes en los que se usa la tecnología *deepfake* para propagar la desinformación y a la par cometer delitos que pueden adquirir connotación social relevante; un ejemplo de aquello es el vídeo creado con

inteligencia artificial en el que el presidente de Ucrania, Volodímir Zelenski, aparentemente ordenaba al ejército y a todo el pueblo ucraniano a rendirse ante Rusia, debido a la guerra (Kardoudi, 2022).

Este es un ejemplo de alta connotación social, sin embargo, existen una gran cantidad de casos en los que aunque la relevancia social no sea tan grande, si existe una notoria gravedad en la comisión de otros delitos; según Deep Trace Technologies, un portal especializado en tecnologías inteligentes y el uso de la inteligencia artificial reveló que el 96% de los 14.600 vídeos *deepfake* online se utilizaron para falsificar material pornográfico no consentido y además, el 90% de estos *deepfakes* son en base a representaciones pornográficas de mujeres (Sandoval et al., 2024).

La comisión de delitos se extiende a niveles insospechados, pues las posibilidades son cada vez más amplias, tanto es así que ya existen casos en los que a través de esta tecnología se han cometidos delitos económicos; uno de ellos es la estafa que quiso realizarse a una empresa energética británica para que transfiriera 220.000 libras a una cuenta bancaria en Hungría, pues a la través de la tecnología *deepfake* se simuló un audio que imitaba la voz del director ejecutivo (Sandoval et al., 2024).

Claramente, esta tecnología podría ser usada con más fines delictivos, por ejemplo, para estafar a hombres o mujeres con fines románticos y lucrativos, a personas de la tercera edad que no están familiarizados con este tipo de tecnología, para casos en los que se puede suplantar la identidad para causar un detrimento a la dignidad y buen nombre de personas o celebridades; todo esto con la enorme ventaja para los ciberdelincuentes que pueden aprovecharse del anonimato que internet les otorga, ya que, incluso este tipo de falsedades profundas se difunden por medio de perfiles falsos creados para ello.

Sin tomar en consideración que incluso este tipo de delitos pueden ser cometidos en territorios recónditos e incluso internacionales, pero que tienen una incidencia directa sobre Ecuador, siendo en esos casos cada vez más complejo perseguir y sobre todo hacer justicia a los autores de estas infracciones. De hecho y de manera

lamentable es una realidad palpable que muchas de estas infracciones penales quedan en la impunidad; ya no por desinterés del Estado, sino por la imposibilidad material de perseguir estos actos.

Confiabilidad y validez de la prueba.

Las *deepfakes* conllevan grandes riesgos, principalmente de tipo ético, político, legal y tecnológico, fundados en la lamentable situación de que reducen o anulan la credibilidad de los documentos audiovisuales (Bañuelos Capistrán, 2020).

A nivel legal, las *deepfakes* suponen un grave riesgo a la tutela judicial efectiva establecida en el artículo 75 de la Constitución de la República del Ecuador (CRE). Este riesgo no solo afecta a los justiciables dentro de un proceso penal en concreto, más bien supone un revés al sistema judicial y su capacidad para resolver estos asuntos con eficiencia, pues el acceso cada vez más fácil, rápido y en masa a estas herramientas supone mayor probabilidad de que se usen las *deepfakes* con fines criminales y, lamentablemente, frente al incremento de la comisión de estas infracciones tenemos a un sistema judicial que en procesos ordinarios no llega a ser célere y en muchos casos efectivo, peor aún cuando se trata de delitos informáticos en los que se necesita de personal altamente capacitado para identificar la generación o manipulación de evidencia con el uso de inteligencia artificial, lo cual resulta casi imposible debido a la deficiencia técnica, tecnológica y de recursos humanos que tiene el Estado dentro del sistema de justicia, pues es relevante recordar que no en todos los cantones se cuenta con unidades de investigación especializadas en delitos informáticos y peor aún de la identificación de *deepfakes.*

Cuando estas *deepfakes* son utilizadas con fines delictivos es imperante gestionar la identificación de la confiabilidad y validez de la prueba; para ello, el elemento de convicción recabado, bajo estricta cadena de custodia debe ponerse en conocimiento del o los profesionales que realizarán la pericia forense correspondiente, misma que permitiría en principio identificar si dicho elemento de convicción eventualmente será una prueba admisible.

Por otro lado, es relevante hacer mención a ciertos momentos en los que la prueba adquiere una mayor atención, ya que, no basta con incorporar un medio probatorio que a juicio del oferente es suficiente, sino que debe cumplir con ciertos requisitos generales, sin los cuales no tendría esa validez; incluso, en otros casos la prueba obtenida es con una más que latente violación a la Constitución, Tratados de Derecho Internacional y la ley en general, siendo así que directamente se constituye como prueba ilegal.

Un ejemplo de este tipo de prueba es aquella derivada de la teoría de los frutos del árbol envenenado, teoría que proviene de su desarrollo anglosajón denominado como *the fruit of the poisonouns tree doctrine.* Dicha teoría prevé que no va a ser posible tener en cuenta una prueba que, aunque se hay obtenido por un medio legítimo, provenga de otro medio que vulnere derechos fundamentales consagrados por la Constitución; así, si el árbol está envenenado, todos sus frutos derivadamente estarán igualmente envenedados.(Goñi Irulegui, 2024)

Un ejemplo podría ser aquel en el que un agente policial obtuvo la confesión de la persona aprehendida por un presunto delito flagrante, a través de ejercer sobre el sujeto actos de tortura o éste fue interrogado sin la presencia de un abogado. Entonces, el testimonio posterior o incluso el acogerse a un procedimiento abreviado en el cual acepta su responsabilidad penal será completamente nulo, pues desde el inicio se obtuvo con violación a los derechos del procesado.

Extrapolando un caso práctico al tema en estudio se puede identificar aquel caso hipotético en el que un fiscal incorpora como prueba dentro de un proceso penal un vídeo en el que se observa a un empresario en una conversación con un tercero admitir que fue partícipe de un esquema de lavado de activos. Este vídeo ha sido creado con tecnología *deepfake*, pues se alteró la voz y la imagen de los interlocutores en ese vídeo, pero la Fiscalía por medio de la investigación realizada a raíz de ese vídeo y solicitar información bancaria y contable del empresario verifica que en efecto hay ciertos rubros que no puede justificarlos adecuadamente, presumiendo la existencia de un lavado de activos. Estos elementos son

incorporados al proceso, pero resulta que a través de la pericial digital forense se logra probar que el vídeo fue creado con tecnología *deepfake.* ¿Qué quiere decir aquello? Pues que el resto de la prueba obtenida será inadmisible por haber contado con la prueba inicial y principal de manera inadecuada, violando la ley; consecuentemente la prueba ulterior será nula.

Admisibilidad probatoria

La norma adjetiva penal, específicamente el artículo 454, numeral 6 del COIP establece que toda prueba o elementos de convicción obtenido con violación a los derechos establecidos en la Constitución, en los Instrumentos Internacionales de Derechos Humanos o en la ley carecen de eficacia probatoria.

Tomando como base dicha afirmación, cualquier elemento generado a partir de la tecnología *deepfake* carecerá de eficacia probatoria, por más apariencia de original que tenga el elemento. Pero la interrogante más difícil de responder es ¿Cómo identificar que la prueba ha sido obtenida con violación a la ley?

He ahí la gran importancia de contar con elementos de convicción lícitos y sobre todo con personal forense y funcionarios judiciales capacitados en estas tecnologías emergentes, a fin de tener la capacidad de identificar un eventual fraude procesal generado a partir del abuso de la inteligencia artificial.

Además, es imperante contar con métodos y tecnología constantemente actualizada que permita verificar más allá de toda duda si un elemento de convicción incorporado al proceso cumple con todos los requisitos de admisibilidad para ser valoradas como prueba en la audiencia de juicio.

En el ámbito nacional ecuatoriano existe el Servicio Nacional de Medicina Legal y Ciencias Forenses (SNMLCF), órgano encargado de prestar sus servicios técnicos científicos en el área de la medicina legal, así como de las ciencias forenses, incluyendo, pero no limitando su acción en cuestiones relativas a Accidentología Vial, Criminalística y otros; todo como la finalidad de que sirvan de apoyo en la búsqueda de la verdad y una correcta administración de justicia.

A más de ello, se resalta la dificultad y en muchas veces confusión a nivel procesal de cómo incorporar la prueba en formato digital dentro de un proceso judicial, ya no solo en el ámbito penal, sino también dentro de otras esferas del Derecho. Es clara la preocupación de muchos profesionales que no conocen de manera profunda y detallada cómo incorporar y evacuar dicha prueba, de ahí que muchos doctrinarios hayan encontrado estos problemas a resolver:

Tabla 1. Propuesta de reforma procesal en Ecuador.

Área a modificar	Situación actual	Modificación que se propone
Procedimientos de recolección y preservación de pruebas digitales.	No existen protocolos claros o unificados para la recolección y preservación de pruebas digitales.	Crear protocolos estandarizados para la recolección, preservación y presentación de pruebas digitales, basados en las mejores prácticas internacionales.
Criterios para la valoración de pruebas digitales.	Criterios generales que no contemplan la complejidad de las pruebas digitales.	Definir criterios específicos que contemplen la complejidad técnica de las pruebas digitales, evaluando autenticidad, integridad y procedencia.
Establecimiento de estándares para la admisibilidad de pruebas electrónicas.	La normativa actual no especifica estándares técnicos claros para la admisibilidad.	Incorporar estándares técnicos claros en el COGEP sobre los requisitos que deben cumplir las pruebas electrónicas para ser admitidas.
Garantías procesales para la autenticidad e integridad de la prueba.	Falta de directrices claras sobre cómo garantizar la autenticidad y la integridad de la prueba durante el proceso judicial.	Establecer procedimientos precisos para garantizar que la cadena de custodia de las pruebas digitales sea inviolable, garantizando autenticidad.

Fuente: https://doi.org/10.33996/revistalex.v7i27.247 (Imaicela Revilla & Alvarado Ajila, 2024)

De estas diferencias procesales y si se establece el foco en el Derecho Procesal Penal, se verifica que existen dos grandes artículos dentro del COIP que deben ser cumplidos a cabalidad para que una prueba digital resulte admisible en un proceso judicial, estos son el artículo 456 y 457, referentes a la cadena de custodia y criterios de valoración, pues solo así se logrará garantizar la legalidad, autenticidad, cadena de custodia y el grado de aceptación científica y técnica que necesariamente requiere este tipo de pruebas.

(…) es muy diferente a que se materialice un documento digital que se podrá notariar ya que es posible con nuestra legislación, pero el notario da fe de que solo existe en alguna página web, y que su contenido que puede ser un escrito digital, imágenes y videos. Es entonces hay que tener en cuenta de que el contenido de esta desmaterialización será solo el físico de la información que está en una página web, en si no es el documento original sino una copia.(Saca-Condo et al., 2023)

Es decir, jamás se podrá hablar que una simple materialización de algún tipo de información digital sea suficiente para probar algún hecho en concreto y menos aún que esto sirva para justificar la responsabilidad penal de una persona, ya que, si la extracción e incorporación de la prueba se lo hace de esa forma, indudablemente se transgrede la cadena de custodia, consecuentemente dicha prueba es inadmisible en todas sus partes.

RESULTADOS

El Servicio Nacional de Medicina Legal y Ciencias Forenses en el ánimo de cumplir su objetivo institucional y estandarizar las actividades para realizar las pericias correspondientes ha creado el *Manual del Subsistema de Investigación Técnico Científica en Materia de Medicina Legal y Ciencias Forenses sobre Peritajes que se llevan a cabo a Nivel Nacional*. Este manual establece un gran número de pericias que durante la investigación de la infracción penal se pueden solicitar y realizar.

Para la investigación de las *deepfakes* no se establece una pericia concreta y especializada que ayude a verificar si determinado elemento ha sido creado con esta tecnología. No obstante, la pericia si cumple con ciertos parámetros o etapas que deben cumplirse para saber que dicha pericia se realiza con un mínimo de estándares, es así que las etapas de peritaje (Aguilar Gualda, 2019) son las siguientes:

- Identificación
- Preservación de material informático objeto de análisis

- Análisis del objeto de investigación
- Emisión y ratificación del dictamen pericial informático

Identificado aquello, el Servicio Nacional de Medicina Legal y Ciencias Forenses establece en el Manual antes aludido un determinado número de pericias afines al análisis de los medios digitales, encontrando que se puede recurrir al uso de pericias tales como:

Identidad de la voz y análisis de señales acústicas, entre las que se incluye:

- Peritaje de análisis y cotejamiento de muestras biométricas de voz para identificar a una persona.
- Peritaje para la determinación, alteraciones, modificaciones o ediciones en una señar acústica.
- Peritaje de análisis, procesamiento y mejoramiento digital de una señal acústica.

Identidad Morfológica y Fisonómica, establecidas como:

- Peritaje de cotejamiento fisonómico y/o morfológico humano entre imágenes, fotografías y/o muestras biométricas.
- Peritaje de cotejamiento morfológico de personas, marcas particulares, objetos y escenarios mediante la fotogrametría.
- Peritaje de composición de rostro de una persona retrato hablado o identikit.
- Peritaje de análisis y cotejamiento de huellas de pies calzado.
- Peritaje de análisis y cotejamiento de la impresión de la banda de rodadura de un neumático.

Ingenierías Informática Forense, que establece las siguientes:

- Peritaje de análisis y materialización del contenido digital, almacenado en fuentes informáticas, equipos, dispositivos y elementos de almacenamiento masivo de datos.
- Peritaje para el estudio de sistemas de información, base de datos e infraestructuras tecnológicas.
- Peritaje de análisis de código malicioso.
- Peritaje para el estudio de cuentas, clientes y servidores de correo electrónico con dominios corporativos o públicos.
- Peritaje para el estudio y análisis de contenido digital registrado y publicado en sitios y páginas web.
- Peritaje de análisis y materialización de datos almacenados en teléfonos celulares, tabletas digitales, teléfonos satelitales, sistemas de navegación GPS, RPAS, smart watch y más tecnología digital de comunicación. (Servicio Nacional de Medicina Legal y Ciencias Forenses, 2022)

Si bien es cierto, el Servicio Nacional de Medicina Legal y Ciencias Forenses a través del Manual aludido determina numerosos tipos de pericias en el ámbito de la informática y uso de medios digitales, no llega a especificar alguna que en concreto identifique o relacione un elemento probatorio con la tecnología *deepfake*.

Esto no quiere decir que a través de las pericias enunciadas previamente no se puede identificar la falsificación o adulteración de un elemento gráfico o sonoro contenido en un medio digital, de hecho, a través de dichas pericias en algunos casos si se logra identificar si existe adulteración o modificación. De hecho, en el eventual caso de que se analice un elemento digital y se logre identificar adulteración en él, inexorablemente dentro del proceso penal se debe respetar la cadena de custodia, a fin de garantizar la autenticidad, identidad e integridad de ese elemento probatorio digital.

El Servicio Nacional de Medicina Legal y Ciencias Forenses pese a contar con varias pericias que se pueden realizar a archivos digitales, en varias ocasiones resulta ser insuficiente. Lamentablemente, este no es un problema exclusivo del sistema de justicia ecuatoriano, pues estas complicaciones se extienden a nivel global y suponen un reto para todos los países.

Precisamente, la imperiosa necesidad de encontrar una solución a este problema ha promovido que grandes entidades internacionales se preocupen por ello y se empiece a desarrollar las denominadas tecnologías de detención de *deepfakes*, entre las que se encuentra la *deepfake* forense.

En 2016 la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) comienza el programa *Media Forensics* (MediFor) para el desarrollo de métodos de análisis digital en medios. En 2018 aparece "FaceForensic" una base de datos de gran escala para entrenar herramientas de detección forense de *deepfake*, con apoyo de Technical University of Munich. (Zeinstra, 2017)

En 2020, Facebook, en alianza con AWS (Amazon Web Services), Microsoft, Partnership on AI's Media Integrity Steering Committee y un grupo de académicos, lanzan el Deepfake Detection Challenge para promover la innovación en técnicas de detección de deepfakes y contenidos mediáticos manipulados, con un premio de 1 millón de dólares (*Deepfake Detection Challenge Dataset*, s. f.)

Reality Defender, una empresa emergente en desarrollar herramientas para detectar *deepfakes* y más contenidos con IA, anunció en octubre del 2023 que a pesar de ser una organización sin ánimo de lucro, debido a la necesidad de contar con recursos pudo recaudar 15 millones de dólares en una ronda de financiación, a fin de destinar a duplicar el pequeño equipo de 23 personas que tenían para así mejorar sus modelos de detección de contenido de inteligencia artificial (Wiggers, 2023).

DISCUSIÓN

La necesidad cada vez más imperiosa de contar con herramientas y mecanismos estatales suficientemente desarrollados para el análisis y validación de los elementos probatorios generados con tecnología informática se hace palpable y urgente. Ecuador, al igual que otros países latinoamericanos están presentando serios problemas en torno a identificación de las *deepfakes*, especialmente en el entorno legal, pues la gravedad y facilidad con la que se puede crear prueba falsa con este tipo de tecnología y sobre todo introducirla en un procedimiento penal trae sin duda retos a los sujetos procesales y en especial a los juzgadores, quienes deben cribar la prueba pertinente y admisible que permita en verdad formar un juicio de valor en torno a la sana crítica, que haga efectiva la tutela judicial efectiva y la administración de justicia.

El Servicio Nacional de Medicina Legal y Ciencias aun contando con algunas pericias informáticas forenses mantiene una desactualización grave respecto a otros países como los europeos y de norte américa, quienes a más de contar con recursos para invertir en este tipo de herramientas tecnológicas de detección de inteligencia artificial, generan convenios con empresas privadas para Meta, Amazon, Microsoft, Nvidia, etc., lo cual evidencia que los países latinoamericanos deberían replicar estos acercamientos con dichas empresas para su aplicación en sus naciones.

Por otro lado, en cuanto a la prueba cabe preguntarse ¿es acaso ahora la prueba digital una garantía de legitimidad y admisible en juicio? Precisamente, para que la prueba digital sea un medio probatorio confiable es necesario contar desde su recolección con medios adecuados que permitan identificar si ésta es legítima, si ésta no ha sido adulterada o incluso creada desde su inicio con tecnología *deepfake*.

La respuesta se encuentra en contar con recursos y mecanismos tecnológicos actualizados en poder del Estado y sobre todo del Servicio Nacional de Medicina Legal y Ciencias Forenses que permita a los justiciables la garantía de que la prueba

obtenida puede ser identificada en su totalidad si ha sido o no creada con inteligencia artificial.

CONCLUSION

Los contenidos audiovisuales y digitales incorporados como prueba dentro de un procedimiento penal deben contar con una atención especial y especializada por parte de los organismos estatales encargados de verificar y certificar que dichos elementos son legítimos, como los que están a disposición del Servicio Nacional de Medicina Legal y Ciencias; organismo que permite realizar pericias en ingeniería informática forense.

La tecnología *deepfake* genera serios perjuicios a diversos niveles y en distintos ámbitos, uno de los más grandes se ubica en la administración de justicia, debido a la incorporación de elementos generados con inteligencia artificial como prueba dentro de un proceso; esto hace indispensable que se establezcan regulaciones en el marco normativo para evitar procesos judiciales viciados o afectados por este tipo de tecnología.

La cooperación interinstitucional de los órganos de administración de justicia, junto a los de criminalística e incluso órganos privados especializados en la detección de tecnología *deepfake* es cada vez más necesaria y urgente, ya que, el Estado al no contar con los recursos suficientes para invertir en este tipo de tecnologías debe apoyarse incluso en órganos de carácter internacional, siendo así posible garantizar una justicia eficaz, protegiendo uno de los derechos más relevantes de nuestra sociedad, conocer la verdad.

FINANCIAMIENTO

No monetario

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A UNIANDES.

REFERENCIAS

Aguilar Gualda, S. de. (2019). *La prueba digital en el proceso judicial: ámbito civil y penal* [Digital evidence in judicial proceedings: civil and criminal scope]. J.M. Bosch Editor. https://elibro.net/es/ereader/uniandesecuador/127045

Bañuelos Capistrán, J. (2020). Deepfake: la imagen en tiempos de la posverdad [Deepfake: image in times of post-truth]. *Revista Panamericana de Comunicación*, 2(1), 51-61. https://www.redalyc.org/articulo.oa?id=664970407007

Coaquira Flores, Á. J. (2025). Los deepfakes y su incidencia en el derecho probatorio [Deepfakes and their impact on evidentiary law]. *Revista Especializada en Investigación Jurídica*, 16, 1-23. https://doi.org/10.20983/reij.2025.1.2

Deepfake Detection Challenge Dataset. (s.f.). *Meta AI*. https://ai.meta.com/datasets/dfdc

Deepfakes: Qué es, tipos, riesgos y amenazas [Deepfakes: What it is, types, risks and threats]. (s.f.). *LISA Institute*. https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

Goñi Irulegui, A. M. (2024). *La prueba electrónica en el entorno digital de la empresa* [Electronic evidence in the digital business environment]. J.M. Bosch Editor. https://elibro.net/es/ereader/uniandesecuador/273822

Imaicela Revilla, J. A., & Alvarado Ajila, L. A. (2024). La incorporación de la prueba digital en el derecho procesal ecuatoriano [The incorporation of digital evidence in Ecuadorian procedural law]. *Revista Lex*, 7(27), 1338-1350. https://doi.org/10.33996/revistalex.v7i27.247

Kardoudi, O. (2022, marzo 17). El primer "deep fake" usado en un conflicto armado muestra a Zelenski rindiéndose [The first "deep fake" used in armed conflict shows Zelensky surrendering]. *El Confidencial*. https://www.elconfidencial.com/tecnologia/novaceno/2022-03-17/hackers-rusos-difunden-un-video-falso-de-zelensky-ordenando-la-rendicion_3393225/

Merino, M. (2019, marzo 31). Conceptos de inteligencia artificial: qué son las GANs o redes generativas antagónicas [Artificial intelligence concepts: what are GANs or generative adversarial networks]. *Xataka*. https://www.xataka.com/inteligencia-artificial/conceptos-inteligencia-artificial-que-gans-redes-generativas-antagonicas

Saca-Condo, H., Marquez-Barreto, A., & Arciniegas-Castro, C. (2023). La inviabilidad de la prueba digital por falta de regulación en los delitos informáticos [The unfeasibility of digital evidence due to lack of regulation in computer crimes]. *593 Digital Publisher CEIT*, 8(4), 21-34. https://doi.org/10.33386/593dp.2023.4.1887

Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review [Amenaza de deepfakes al sistema de justicia criminal: una revisión sistemática]. *Crime Science*, 13(1), 41. https://doi.org/10.1186/s40163-024-00239-1

Servicio Nacional de Medicina Legal y Ciencias Forenses. (2022). *Manual del Subsistema de Investigación Técnico Científica en Materia de Medicina Legal y Ciencias Forenses sobre Peritajes* [Manual of the Technical Scientific Investigation Subsystem on Legal Medicine and

Forensic Sciences Expert Reports]. https://www.cienciasforenses.gob.ec/wp-content/uploads/2023/04/MANUAL-PERITAJES-SITC-FINAL-2022.pdf

Wiggers, K. (2023, octubre 17). Reality Defender raises $15M to detect text, video and image deepfakes [Reality Defender recauda $15M para detectar deepfakes de texto, video e imagen]. *TechCrunch*. https://techcrunch.com/2023/10/17/reality-defender-raises-15m-to-detect-text-video-and-image-deepfakes/

Zeinstra, C. (2017). *Forensic face recognition: from characteristic descriptors to strength of evidence* [Reconocimiento facial forense: de descriptores característicos a fuerza de evidencia] [Tesis doctoral, University of Twente]. https://doi.org/10.3990/1.9789036543750