Polo del Conocimiento

Pol. Con. (Edición núm. 102) Vol. 10, No 1
Enero 2025, pp. 1742-1775
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v10i1.8778

La importancia de la prueba digital en los procedimientos penales en Ecuador

The importance of digital evidence in criminal procedures in Ecuador

A importância das provas digitais nos processos penais no Equador

César Eugenio Navas-Abad [I]
cesar.navas.47@est.ucacue.edu.ec
https://orcid.org/0009-0008-3950-5643

David Sebastián Vázquez-Martínez [II]
david.vazquez@ucacue.edu.ec
https://orcid.org/0000-0002-7430-0351

Correspondencia: cesar.navas.47@est.ucacue.edu.ec

Ciencias Sociales y Políticas
Artículo de Investigación

*** Recibido:** 17 de noviembre de 2024 ***Aceptado:** 06 de diciembre de 2024 *** Publicado:** 17 de enero de 2025

I. Universidad Católica de Cuenca, Azuay, Ecuador.
II. Universidad Católica de Cuenca, Azuay, Ecuador.

Resumen

La prueba digital ha emergido como un componente en los procedimientos penales modernos debido al crecimiento de delitos informáticos y avances tecnológicos. En Ecuador, aunque el Código Orgánico Integral Penal (COIP) reconoce su validez, la ausencia de una regulación específica y adecuada limita su efectiva aplicación en el sistema judicial. La falta de protocolos claros y los problemas técnicos en autenticación y cadena de custodia dificultan la validez y fiabilidad de la evidencia digital. Este problema destaca la necesidad urgente de reformar las normativas y procedimientos para alinearse con estándares internacionales, como la norma ISO 27002:2013. La implementación de una metodología basada en tecnologías de la información y comunicación (TICS) para mejorar la gestión de pruebas digitales es esencial. Los objetivos incluyen identificar deficiencias en el COIP, analizar el uso y regulación de la prueba digital en Ecuador y comparar los procedimientos nacionales con los estándares internacionales para garantizar una justicia precisa y efectiva.

Palabras Clave: prueba digital; derecho procesal penal; derecho probatorio; derecho digital; tecnologías de información y comunicación.

Abstract

Digital evidence has emerged as a component in modern criminal procedures due to the growth of cybercrimes and technological advances. In Ecuador, although the Comprehensive Organic Penal Code (COIP) recognizes its validity, the absence of specific and adequate regulation limits its effective application in the judicial system. The lack of clear protocols and technical problems in authentication and chain of custody hinder the validity and reliability of digital evidence. This issue highlights the urgent need to reform regulations and procedures to align with international standards, such as ISO 27002:2013. The implementation of a methodology based on information and communication technologies (ICT) to improve the management of digital evidence is essential. Objectives include identifying deficiencies in the COIP, analyzing the use and regulation of digital evidence in Ecuador, and comparing national procedures with international standards to ensure accurate and effective justice.

Keywords: digital proof; criminal procedural law; evidentiary law; digital right; information and communication technologies.

Resumo

As provas digitais surgiram como um componente dos processos penais modernos devido ao crescimento dos crimes cibernéticos e aos avanços tecnológicos. No Equador, embora o Código Penal Orgânico Integral (COIP) reconheça a sua validade, a ausência de regulamentação específica e adequada limita a sua aplicação efetiva no sistema judicial. A falta de protocolos claros e os problemas técnicos na autenticação e na cadeia de custódia prejudicam a validade e a fiabilidade das provas digitais. Esta questão destaca a necessidade urgente de reformar regulamentos e procedimentos para se alinharem com as normas internacionais, como a ISO 27002:2013. A implementação de uma metodologia baseada em tecnologias de informação e comunicação (TIC) para melhorar a gestão de provas digitais é essencial. Os objetivos incluem identificar deficiências no COIP, analisar o uso e a regulamentação de provas digitais no Equador e comparar os procedimentos nacionais com os padrões internacionais para garantir uma justiça precisa e eficaz.

Palavras-chave: prova digital; direito processual penal; direito probatório; direito digital; tecnologias de informação e comunicação.

Introducción

La prueba digital ha adquirido un papel central en los procedimientos penales contemporáneos, particularmente en Ecuador, donde el aumento de los delitos informáticos y la creciente dependencia de tecnologías digitales presentan un desafío significativo para el sistema judicial. Sin embargo, su incorporación enfrenta obstáculos debido a la ausencia de un marco normativo específico que regule de manera clara su manejo, autenticidad y validez en los tribunales. A pesar de que el Código Orgánico Integral Penal (COIP, 2023) y el Código Orgánico General de Procesos (2015) reconocen la prueba digital como válida, su implementación se ve limitada por deficiencias en los procedimientos técnicos, como la cadena de custodia y la autenticación de las pruebas, lo que genera incertidumbre sobre su fiabilidad en los procesos judiciales.

Este problema es de vital importancia, ya que la falta de un uso adecuado y confiable de la prueba digital afecta la capacidad del sistema penal para responder eficazmente a los delitos, tanto tradicionales como cibernéticos. La evidencia digital es esencial para probar conductas delictivas que involucran tecnología, y su correcta aplicación es fundamental para garantizar la justicia y la seguridad en el país. La falta de regulación precisa puede comprometer no solo la validez de la

prueba en sí, sino también derechos fundamentales, como la presunción de inocencia y el debido proceso.

Uno de los casos más notables donde la prueba digital fue decisiva es el caso "Sobornos 2012-2016". En este proceso, se utilizaron correos electrónicos y registros de transferencias bancarias para demostrar un esquema de sobornos que involucraba a altos funcionarios del gobierno y empresarios, incluyendo al expresidente Rafael Correa. La autenticidad e integridad de estas pruebas digitales fueron verificadas mediante peritajes informáticos, lo que permitió su admisión en el juicio y contribuyó a la condena de varios implicados. Otro ejemplo relevante es el caso de corrupción en Petroecuador. Aquí, la evidencia digital, como correos electrónicos, mensajes de texto y registros de llamadas, fue crucial para demostrar la existencia de sobornos y corrupción en la adjudicación de contratos. Los fiscales utilizaron peritajes técnicos para validar la autenticidad de los mensajes y rastrear la cadena de custodia de las pruebas digitales (Quichimbo et al., 2024).

En ese sentido, la prueba digital se enmarca en los conceptos de autenticidad, integridad y fiabilidad, los cuales son indispensables para su admisibilidad en los procesos judiciales. La autenticidad de la prueba digital se refiere a la capacidad de demostrar que los datos no han sido alterados desde su recolección, mientras que la integridad asegura que se ha mantenido la totalidad de los datos. Estas características son esenciales para que la prueba sea admisible en un juicio. La fiabilidad, por otro lado, está relacionada con la capacidad de garantizar que la evidencia puede ser reproducida y verificada por peritos independientes, lo cual es crucial para respetar el principio de contradicción, que asegura que ambas partes en un proceso puedan cuestionar la prueba presentada.

Por su parte, Martínez (2022) subraya la necesidad urgente de que el derecho penal adapte sus enfoques tradicionales ante la revolución tecnológica. Según su análisis, la integración de la prueba digital en los procedimientos judiciales no es una opción, sino una necesidad impuesta por el avance de la tecnología, tanto en los delitos informáticos como en los delitos tradicionales, donde la evidencia digital juega un papel cada vez más relevante. Sin embargo, esta transición no está exenta de desafíos, ya que plantea preguntas fundamentales sobre la validez de la prueba y el respeto a los derechos fundamentales de los procesados. Martínez argumenta que la rápida evolución de la tecnología exige que todos los actores involucrados en el sistema judicial, desde jueces hasta abogados y fiscales, se adapten a los nuevos retos que supone el manejo de la evidencia digital.

Precisamente, las estadísticas revelan la creciente importancia de la prueba digital en el sistema judicial ecuatoriano. Concretamente, entre enero y agosto de 2020, se registraron 5,048 denuncias por delitos informáticos en Ecuador, en ese contexto, los tres principales delitos informáticos fueron: (i) suplantación de identidad: 2,162 casos (42.83%), (ii) falsificación y uso de documento falso: 1,448 casos (28.68%), (iii), apropiación fraudulenta por medios electrónicos: 1,033 casos (20.46%). Estos tres delitos representaron el 92% de todos los casos reportados, subrayando la importancia de la evidencia digital en la persecución de estos crímenes (Sarmiento & Maldonado, 2024).

Por su parte, González (2021) analiza cómo la revolución digital ha generado nuevos retos para el derecho penal, especialmente en lo que se refiere a la prueba derivada de delitos informáticos. Según su estudio, la doctrina y jurisprudencia penal española establecen que para que una prueba sea lícita, debe ser presentada con todas las garantías procesales que permitan su contradicción. Es aquí donde la pericia informática adquiere un rol crucial. Los expertos en informática forense son esenciales para confirmar o refutar la autenticidad y validez de la evidencia digital, actuando como garantes de que esta prueba ha sido obtenida y preservada adecuadamente. La intervención de peritos especializados en tecnología no solo asegura que la prueba cumpla con los requisitos de autenticidad e integridad, sino que también respalda la transparencia del proceso, al permitir que las partes puedan controvertir la prueba de manera efectiva.

Adicionalmente, surgen una serie de interrogantes que reflejan la necesidad de realizar una revisión profunda del marco jurídico en Ecuador respecto a la prueba digital. Uno de los principales desafíos que enfrenta el sistema judicial ecuatoriano es la falta de protocolos estandarizados para la recolección y preservación de la evidencia digital. La inexistencia de una normativa clara sobre cómo debe gestionarse esta evidencia genera un vacío que puede ser aprovechado por las defensas para cuestionar su validez en los tribunales. En los procesos penales, donde el principio de legalidad y la presunción de inocencia son pilares fundamentales, cualquier duda sobre la autenticidad de la prueba puede comprometer todo el procedimiento, afectando gravemente la búsqueda de justicia (Porras, 2023).

Además, el rápido avance de la tecnología plantea la necesidad de una capacitación constante para los operadores del sistema judicial. Jueces, fiscales, abogados y peritos deben mantenerse actualizados sobre las nuevas herramientas y métodos para la recolección y análisis de pruebas digitales. De lo contrario, existe el riesgo de que la evidencia sea manipulada o malinterpretada, lo

que podría llevar a fallos judiciales injustos. En este sentido, es indispensable que el sistema judicial ecuatoriano no solo implemente reformas normativas, sino que también invierta en la formación y especialización de sus operadores en temas de tecnología y derecho digital.

El problema de investigación se centra en las limitaciones y desafíos que enfrenta el sistema judicial ecuatoriano para garantizar la admisibilidad y validez de la prueba digital en los procesos penales. Si bien el COIP y el Código Orgánico General de Procesos reconocen la validez de la evidencia digital, persisten deficiencias técnicas y normativas, tales como la ausencia de protocolos estandarizados y procedimientos específicos que aseguren la autenticidad, integridad y fiabilidad de dicha prueba.

Conforme a ello, se plantea que el sistema judicial ecuatoriano podría mejorar la admisibilidad y validez de la prueba digital en los procesos penales mediante el establecimiento de un marco normativo claro y específico, que incluya protocolos de autenticación y cadena de custodia, así como la capacitación continua de jueces, fiscales y peritos en tecnología forense. A tales efectos, surge como pregunta de investigación ¿Cómo puede el sistema judicial ecuatoriano mejorar la admisibilidad y validez de la prueba digital en los procesos penales? Asimismo, el objetivo general de esta investigación será analizar los desafíos actuales en la implementación de la prueba digital en el sistema penal ecuatoriano y proponer soluciones para mejorar su admisibilidad y uso eficaz en los procedimientos judiciales.

Como primer objetivo específico, se busca identificar las principales deficiencias técnicas y normativas en el uso de la prueba digital en Ecuador. Por otro lado, se aspira analizar la aplicación práctica de los protocolos relacionados con la autenticación y la cadena de custodia de pruebas digitales, además, como tercer objetivo, se plantea proponer reformas y buenas prácticas que fortalezcan la implementación de la prueba digital en el sistema judicial del país. Asimismo, se sugiere la creación de protocolos técnicos estándar para la recolección y preservación de pruebas digitales, así como la implementación de un sistema de certificación para peritos informáticos, inspirado en modelos internacionales como el de España o Estados Unidos, donde la evidencia digital es gestionada de manera más efectiva en los procesos judiciales.

Desarrollo

Concepto y características de la prueba digital

La prueba electrónica es cualquier tipo de dato (generado, almacenado o transmitido) que se haya obtenido mediante el uso de dispositivos electrónicos, que haya sido utilizado en un proceso judicial para sustentar hechos significativos. Esta información incluye una amplia gama de formatos, desde correos electrónicos, mensajes de texto, imágenes y videos, hasta archivos digitales y datos complejos almacenados en bases de datos. Incluso con el avance de las tecnologías en la nube, la evidencia puede incluir información almacenada en servidores remotos, lo que ha agregado una nueva capa de complejidad en términos de jurisdicción y acceso a la evidencia (López, 2023). La prueba electrónica se ha convertido en un elemento clave dentro del derecho procesal contemporáneo, lo que refleja el creciente uso de las tecnologías digitales en la vida cotidiana y, en consecuencia, en las disputas judiciales. La prueba digital es una fuente importante de evidencia en el contexto de un mundo interconectado y en rápido crecimiento basado en dispositivos electrónicos, ya que proporciona un rastro detallado y verificable de interacciones, transacciones y eventos, que pueden desempeñar un papel primordial en la conclusión de disputas legales. Este tipo de evidencia no solo ha transformado la forma en que se llevan a cabo los litigios, sino que también ha creado nuevos problemas y posibilidades para el sistema judicial.

Con el auge de los dispositivos móviles y las redes sociales, las interacciones que antes se realizaban en persona o a través de la correspondencia tradicional ahora ocurren en entornos digitales. Los mensajes de WhatsApp, los correos electrónicos, las publicaciones en redes como Facebook o Twitter, e incluso las grabaciones de cámaras de vigilancia digitalizadas o sistemas de videoconferencia, se han convertido en pruebas cruciales en casos civiles, penales y administrativos. La evidencia electrónica se ha convertido en una parte tan común del proceso judicial que es casi imposible imaginar un proceso judicial sin algún tipo de evidencia digital (Vázquez, 2022).

La noción de evidencia electrónica engloba varios tipos y fuentes. Las más frecuentes son las imágenes y los videos digitales, que son recursos visuales que proporcionan un registro inmediato de eventos o contextos que son pertinentes para el caso. En la medida de los ejemplos (por ejemplo, lesión o accidente), una imagen o un video tomado por una cámara de seguridad puede ser muy importante no solo para la cronología de los eventos, sino también para determinar la responsabilidad entre las partes.

Pol. Con. (Edición núm. 102) Vol. 10, No 1, Enero 2025, pp. 1742-1775, ISSN: 2550 - 682X

Importancia de la prueba digital en el proceso penal

Como señala Martínez (2022), la era electrónica ha incrementado la demanda de aplicación de la prueba digital para la prueba de los delitos, ya sea convencional o cibernética. Esta realidad exige una revisión urgente de los enfoques tradicionales en el derecho penal, ya que la integración de la prueba digital plantea cuestiones fundamentales sobre su validez y el respeto a derechos fundamentales como la legalidad y la presunción de inocencia. Martínez destaca que "todos los operadores jurídicos" deben participar en el proceso de adaptación a esta realidad tecnológica tan rápidamente progresiva y disruptiva.

Por otro lado, González (2021) ha analizado, en este sentido, los nuevos retos que plantea al derecho la revolución digital en el ámbito de la prueba de los delitos informáticos. La investigación señala que, en lo que respecta a la doctrina y jurisprudencia penal española, para que una prueba sea reconocida como lícita ha de demostrarse con las condiciones que garanticen su contradicción. Las habilidades informáticas son muy importantes en la evaluación de la validez de estas pruebas y, en consecuencia, sirven como prueba crítica en el tribunal penal.

Por otra parte, Porras (2023), sostiene que gracias al rápido desarrollo de las tecnologías, se ha incorporado al ordenamiento jurídico colombiano un nuevo campo de soluciones probatorias. Si bien, mientras tanto, existe una regulación para el uso de las tecnologías, la admisión de la prueba digital en los procesos judiciales aún no ha sido regulada de manera clara. Esta ausencia de lineamientos y experticia ha puesto en juego los desafíos de cómo los abogados y los administradores de justicia pueden evaluar esta prueba, pues su invalidez puede llevar a la vulneración de derechos fundamentales y al descarte de pruebas relevantes.

Con el desarrollo de las tecnologías de la información y la comunicación, el ámbito del derecho penal ha cambiado drásticamente al otorgarle un papel cada vez más importante a la prueba digital. Este acontecimiento también impone a los operadores judiciales la exigencia de reconfigurar sus herramientas de valoración no solo en lo que respecta a la prueba ordinaria, sino a la prueba proveniente de medios electrónicos y digitales. Por tanto, la prueba digital se define como toda información electrónica creada y conservada en un formato digital de la que se pueden extraer datos y convertirlos en datos susceptibles de análisis. Esta información es sometida a un examen especializado por parte de peritos, quienes elaboran un informe detallado que se incorpora al proceso judicial (López, 2023).

La implementación de la prueba digital en los procesos penales genera una serie de desafíos que exigen un método muy cuidadoso y detallado. Uno de los principales problemas es la obtención de esta prueba. La prueba digital puede obtenerse por los siguientes medios, como por ejemplo en el caso de la observación secreta, que pone en duda su fundamento jurídico y su admisibilidad en juicio. Es fundamental determinar si el procedimiento para llegar a ella se ajusta a las normas jurídicas y, en lo que respecta a los hechos, es compatible con los derechos fundamentales de las partes afectadas. Otro aspecto crítico es la admisibilidad de la prueba digital. Es imperativo establecer criterios para definir de forma clara y precisa el momento en que la prueba digital es válidamente admisible en el proceso penal. Estos criterios deben garantizar que la prueba digital sea pertinente (es decir, relevante para el caso) y confiable (es decir, atribuible al acusado o con certeza de ser admisible en el tribunal) y que haya sido producida legalmente para no ser excluida del proceso judicial (Magro, 2020).

La evaluación de la prueba digital representa otro desafío importante. Los jueces deben recibir una formación integral para evaluar adecuadamente la prueba digital, tanto técnica como legalmente. Comprender el proceso mediante el cual se ha obtenido, procesado y comunicado la prueba es fundamental para una interpretación adecuada y para realizar una evaluación justa e imparcial (Porras, 2023).

Regulación específica de la prueba digital en el COIP

Según el COIP (2023) y el artículo 456, el término “cadena de custodia” se utiliza para ilustrar tanto los componentes materiales como las evidencias digitales utilizadas en la prueba. El objetivo de esta cadena es verificar la autenticidad de dichos elementos probatorios, verificando su identidad y manteniendo la condición original de estos elementos durante toda la cadena de actividades, desde su recolección y traslado, manipulación y análisis, hasta su conservación. También es importante que se registren las condiciones y las personas que participan en cada etapa de la manipulación de estos componentes (y, cuando sea posible, los cambios que realicen los custodios) para que la investigación pueda optimizarse para diferentes contextos.

El procedimiento de cadena de custodia comienza y termina en el mismo lugar en que se recolecta o encuentra la evidencia, y solo puede cerrarse mediante orden de la autoridad competente. Este proceso abarca a diferentes actores, como los especialistas del personal del sistema de investigación integral comisionada, los peritos en medicina legal y los profesionales de las ciencias forenses, los funcionarios especializados en tránsito y todas las personas en funciones públicas o privadas, de

alguna manera, vinculadas a estos elementos. Ello incluye también a los profesionales de la salud, como aquellos que puedan tener exposición a potenciales evidencias relacionadas con la investigación. El artículo 460 señala que el reconocimiento de la escena del delito es asunto de responsabilidad del fiscal acompañado de un equipo especializado. Este equipo podrá estar integrado por expertos en investigación, medicina forense, ciencias forenses o, cuando sea necesario, personal competente en materia de tránsito. Estos exámenes no se restringen al espacio físico, sino que también incluyen el "espacio digital", los servicios digitales, los medios electrónicos, así como la tecnología, que son fundamentales para la investigación. Este apartado se refiere al papel del mundo digital en las investigaciones criminales contemporáneas, extendiendo la investigación a los espacios virtuales.

Como lo indica el artículo 499, todo contenido digital será admisible como prueba documental siempre que se ajuste a lo dispuesto en este Reglamento. Asimismo, el artículo 500 redefine el concepto de contenido digital, entendiéndolo como toda representación informática que permita reflejar hechos, datos o ideas de la realidad, susceptibles de ser procesados, almacenados o transmitidos a través de tecnologías diseñadas para el procesamiento informático. En el marco de las investigaciones, el proceso de análisis, evaluación, recuperación y presentación de este contenido digital, almacenado en dispositivos o sistemas informáticos, se realizará mediante técnicas forenses digitales, con el fin de garantizar la integridad y autenticidad de la información obtenida.

En el caso de que el contenido digital se encuentre almacenado en sistemas dinámicos, en soportes de memoria y en aparatos tecnológicos que sean centrales en las infraestructuras globales y locales de los sectores público o privado, la investigación forense digital de dicho contenido deberá realizarse in situ y en tiempo real. Esto garantiza la integridad de la muestra y es la base de una cadena de custodia que permite su posterior evaluación y análisis. Si la evidencia digital se encuentra almacenada en soportes no volátiles, se emplearán métodos forenses digitales para recuperar la evidencia, preservándola en su totalidad y manteniendo la cadena de custodia.

Además, durante una investigación, registro o allanamiento, es primordial prestar especial atención a cualquier dispositivo físico utilizado para el almacenamiento, procesamiento o transmisión de información digital. Cada objeto deberá ser cuidadosamente identificado y documentado de manera que se pueda determinar su posición exacta (verificada mediante fotografías y un plano comentado del entorno). Luego deberá ser trasladado con las máximas medidas de seguridad a un centro

especializado, donde se le garantizará su protección y al mismo tiempo su disponibilidad para el proceso judicial.

Convenios Internacionales aplicables

El Convenio de Budapest sobre la Ciberdelincuencia (2001) y su Segundo Protocolo Adicional (2023) proporcionan un marco amplio y detallado para que los Estados miembros puedan gestionar adecuadamente la ciberdelincuencia y fortalecer la cooperación internacional en la investigación y el enjuiciamiento de dichos delitos. Este Convenio, que es líder en su campo, tiene por objeto ofrecer una forma de estructura clara y unificada que permita a los Estados signatarios actuar mediante mecanismos legislativos y operativos para contrarrestar las crecientes amenazas que surgen en el ciberespacio.

El artículo 14, parte del Título 1, sobre disposiciones generales, analiza el ámbito de aplicación de los mecanismos de derecho en los procesos penales. La obligación exige que los Estados signatarios establezcan las normas necesarias para otorgar de forma clara y crítica a sus organismos poderes adecuados para la investigación de la ciberdelincuencia y capaces de relacionarse con las pruebas producidas en el mundo electrónico. Esta demanda de un buen marco legislativo se ve satisfecha por el aumento de la ciberdelincuencia, que es transnacional y, cuando corresponde, se ve facilitada por los sistemas y redes informáticas utilizados para una variedad de delitos.

En consecuencia, la Convención no sólo se aplica a los delitos individuales enumerados en sus artículos 2 a 11 (por ejemplo, acceso ilícito a sistemas informáticos, interferencia con datos y sistemas, producción y distribución de pornografía infantil), sino también a cualquier otro delito penal cometido mediante canales digitales o sistemas informáticos, asegurando así el máximo alcance regulatorio. Además, el archivo de pruebas electrónicas se aborda, según el delito de que se trate, de una manera que garantiza que los procedimientos penales puedan basarse en pruebas materiales y adecuadas en la era digital.

Por otra parte, el Segundo Protocolo Adicional posterior a la Convención, en particular el artículo 12, establece un enfoque de colaboración directa entre las autoridades nacionales de los dos países mediante equipos conjuntos de investigación y la posibilidad de investigaciones conjuntas. Se trata de una parte vital de esta disposición en el contexto de la ciberdelincuencia, ya que estos delitos suelen ser de naturaleza transnacional y, por lo tanto, se dirigen a más de una jurisdicción.

Al permitir la formación de equipos conjuntos, el Protocolo busca permitir que los Estados trabajen juntos para coordinar la recopilación de pruebas, intercambiar información y, en última instancia,

procesar a los responsables de manera más efectiva y rápida. Sin embargo, a los efectos de preservar la soberanía del Estado y el derecho de las personas, se aplican restricciones y criterios al uso de la información y las pruebas obtenidas en el marco de dichos acuerdos de cooperación.

El artículo 12 establece que el uso de las pruebas y la información proporcionadas por una Parte a otra puede restringirse o denegarse de conformidad con las condiciones acordadas en el acuerdo de cooperación. Si no existen condiciones explícitamente definidas en el contrato, los Estados pueden explotar la información que se haya recopilado para los fines originalmente asignados, con o sin el permiso explícito de la Parte de la que se haya recibido la información, para la investigación y el enjuiciamiento de otros delitos.

Esta autorización no es necesaria en el caso de que las normas básicas del derecho del Estado receptor impongan el uso de la información para salvaguardar los derechos del acusado, es decir, una salvaguardia procesal. Además, el Protocolo permitirá cualquier aplicación de la información, incluso en situaciones de emergencia, en cuyo caso la Parte receptora informará inmediatamente, sin demora, a quien emitió la información y a la autoridad competente. Esta tensión en la aplicación de las pruebas tiene por objeto encontrar una solución de compromiso entre la eficiencia de la coordinación internacional y la garantía de la dignidad y los derechos de cada Estado.

Normas ISO

El Convenio de Budapest sobre la Ciberdelincuencia (2001) y su Segundo Protocolo Adicional (2023) proporcionan un marco amplio y detallado para que los Estados miembros puedan gestionar adecuadamente la ciberdelincuencia y fortalecer la cooperación internacional en la investigación y el enjuiciamiento de dichos delitos. Este Convenio, que es líder en su campo, tiene por objeto ofrecer una forma de estructura clara y unificada que permita a los Estados signatarios actuar mediante mecanismos legislativos y operativos para contrarrestar las crecientes amenazas que surgen en el ciberespacio.

El artículo 14, parte del Título 1, sobre disposiciones generales, analiza el ámbito de aplicación de los mecanismos de derecho en los procesos penales. La obligación exige que los Estados signatarios establezcan las normas necesarias para otorgar de forma clara y crítica a sus organismos poderes adecuados para la investigación de la ciberdelincuencia y capaces de relacionarse con las pruebas producidas en el mundo electrónico. Esta demanda de un buen marco legislativo se ve satisfecha por el aumento de la ciberdelincuencia, que es transnacional y, cuando corresponde, se ve facilitada por los sistemas y redes informáticas utilizados para una variedad de delitos.

En consecuencia, la Convención no sólo se aplica a los delitos individuales enumerados en sus artículos 2 a 11 (por ejemplo, acceso ilícito a sistemas informáticos, interferencia con datos y sistemas, producción y distribución de pornografía infantil), sino también a cualquier otro delito penal cometido mediante canales digitales o sistemas informáticos, asegurando así el máximo alcance regulatorio. Además, el archivo de pruebas electrónicas se aborda, según el delito de que se trate, de una manera que garantiza que los procedimientos penales puedan basarse en pruebas materiales y adecuadas en la era digital.

Por otra parte, el Segundo Protocolo Adicional posterior a la Convención, en particular el artículo 12, establece un enfoque de colaboración directa entre las autoridades nacionales de los dos países mediante equipos conjuntos de investigación y la posibilidad de investigaciones conjuntas. Se trata de una parte vital de esta disposición en el contexto de la ciberdelincuencia, ya que estos delitos suelen ser de naturaleza transnacional y, por lo tanto, se dirigen a más de una jurisdicción.

Al permitir la formación de equipos conjuntos, el Protocolo busca permitir que los Estados trabajen juntos para coordinar la recopilación de pruebas, intercambiar información y, en última instancia, procesar a los responsables de manera más efectiva y rápida. Sin embargo, a los efectos de preservar la soberanía del Estado y el derecho de las personas, se aplican restricciones y criterios al uso de la información y las pruebas obtenidas en el marco de dichos acuerdos de cooperación.

El artículo 12 establece que el uso de las pruebas y la información proporcionadas por una Parte a otra puede restringirse o denegarse de conformidad con las condiciones acordadas en el acuerdo de cooperación. Si no existen condiciones explícitamente definidas en el contrato, los Estados pueden explotar la información que se haya recopilado para los fines originalmente asignados, con o sin el permiso explícito de la Parte de la que se haya recibido la información, para la investigación y el enjuiciamiento de otros delitos.

Esta autorización no es necesaria en el caso de que las normas básicas del derecho del Estado receptor impongan el uso de la información para salvaguardar los derechos del acusado, es decir, una salvaguardia procesal. Además, el Protocolo permitirá cualquier aplicación de la información, incluso en situaciones de emergencia, en cuyo caso la Parte receptora informará inmediatamente, sin demora, a quien emitió la información y a la autoridad competente. Esta tensión en la aplicación de las pruebas tiene por objeto encontrar una solución de compromiso entre la eficiencia de la coordinación internacional y la garantía de la dignidad y los derechos de cada Estado.

La continua evolución de las tecnologías y el auge de nuevos tipos de delitos cibernéticos, como la ciber extorsión y los fraudes electrónicos, ha llevado al desarrollo de procedimientos forenses específicos para diferentes tipos de dispositivos y plataformas. Por ejemplo, en el caso de los teléfonos móviles Android, se están creando protocolos de investigación detallados que incluyen la recolección de datos de aplicaciones, comunicaciones en redes sociales, historial de navegación, entre otros, que pueden ser clave para resolver delitos relacionados con el crimen digital. Estos procedimientos no solo actualizan las metodologías tradicionales de análisis forense, sino que también incorporan nuevas herramientas tecnológicas para adaptarse a los cambios rápidos en el panorama digital (Banegas & Andrade, 2022).

Además, el avance hacia la digitalización de la evidencia en otros ámbitos, como la recolección de datos en la nube o el análisis de grandes volúmenes de datos (big data), plantea nuevos desafíos en términos de preservación, análisis y interpretación de la evidencia. El marco normativo debe estar en constante actualización para abordar estos retos y garantizar que las metodologías forenses continúen siendo eficaces y legalmente válidas. De este modo, la norma ISO/IEC 27037:2012 y otros estándares relacionados no solo facilitan el trabajo de los peritos forenses y los investigadores, sino que también aseguran que la justicia se administre de manera transparente y conforme a los principios del debido proceso.

La norma ISO/IEC 27041:2015 (2015) cumple un papel central en el ámbito de la gestión de evidencia digital, ya que establece pautas detalladas para documentar y validar los métodos de análisis empleados en el manejo de dicha evidencia. La norma tiene como propósito no solo orientar sobre los aspectos técnicos de la investigación digital, sino también fortalecer la credibilidad de estos procesos en un entorno judicial donde cada método debe ser defendible y reproducible.

Al proporcionar una estructura estándar, la ISO/IEC 27041:2015 asegura que cualquier análisis realizado sobre evidencia digital puede ser replicado por otros expertos y supervisado en detalle, lo cual es esencial para evitar errores y prejuicios que podrían comprometer los resultados. Esta capacidad de replicación y defensa de los métodos empleados es vital en litigios, pues permite que la evidencia sea aceptada con confianza en tribunales, manteniendo así su peso y fiabilidad. Además, la normativa establece una serie de requisitos y recomendaciones para la correcta documentación, garantizando que todos los pasos y decisiones del proceso de análisis estén registrados de manera rigurosa, lo cual refuerza la transparencia y la trazabilidad de los hallazgos.

La ISO/IEC 27042:2015 (2015), por su parte, ofrece un enfoque exhaustivo en el análisis e interpretación de la evidencia digital. Esta norma establece un conjunto de procedimientos orientados a guiar a los expertos en todas las etapas de una investigación digital, desde la identificación inicial de la evidencia hasta su adecuada presentación en juicio. En un contexto donde la cadena de custodia es fundamental, esta norma se centra en mantener la integridad de la evidencia durante todo el proceso, asegurando que cada paso esté documentado y que todos los involucrados sigan procedimientos estandarizados.

Esto no solo permite que los hallazgos sean sólidos, sino que también ayuda a evitar posibles ataques o cuestionamientos en juicio, ya que toda la evidencia se analiza con base en métodos rigurosos y bien definidos. Al establecer una metodología clara, la norma también facilita la comprensión de los hallazgos por parte de jueces y abogados que quizás no tengan experiencia técnica, lo cual es crucial para que la evidencia digital sea utilizada de forma efectiva en los procesos judiciales.

En cuanto a la norma ISO/IEC 27043:2015 (2015), esta se ocupa del proceso global de investigación forense digital, definiendo un marco amplio que permite entender y estandarizar la forma en que se deben llevar a cabo las investigaciones que implican evidencia digital. Su enfoque integral incluye directrices para abordar no solo los aspectos comunes de una investigación digital, sino también cómo enfrentar situaciones excepcionales que puedan surgir durante el proceso.

La norma también ha contribuido a desarrollar un proceso investigativo ágil y escalable, que se acomode a los requerimientos de un mundo jurídico conectado. De esta manera, no solo se asegura la calidad de la evidencia digital, sino que también se promueve la interacción entre agencias o jurisdicciones, mejorando así la distribución de la información y aumentando las posibilidades de una buena investigación a escala internacional.

La norma ISO/IEC 27037:2012 (2012) constituye la referencia fundamental en la gestión de la evidencia digital, y en ella se basan todos los trabajos que se realizan en este campo. Esta norma proporciona una serie de protocolos específicos para la gestión de la evidencia digital que abordan etapas importantes, entre ellas la identificación, recolección, extracción y protección de dicha evidencia. Estos principios no solo definen las bases de la investigación digital, sino que también aseguran que cualquier proceso relacionado con la recolección y uso de evidencia digital sea formal y riguroso, cumpliendo con los estándares internacionales.

Por otra parte, las directrices generales que proporciona la norma ISO/IEC 27037:2012:2012 no sólo se aplican a la evidencia digital, sino que también incluyen los procedimientos para la adquisición de evidencia no digital, aspecto que es importante para el análisis de la evidencia digital. La norma tiene como objetivo ofrecer orientación a quienes tienen el control sobre la gestión de la evidencia digital, por ejemplo, los primeros intervinientes en la respuesta a la evidencia digital (DEFR), los especialistas en evidencia digital (DES), otro personal de respuesta a incidentes y los directores de laboratorios forenses. El objetivo es garantizar que estas personas actúen de acuerdo con las mejores prácticas reconocidas mundialmente, asegurando que la investigación se lleve a cabo de manera sistemática e imparcial, al tiempo que se preserva la autenticidad e integridad de la evidencia.

Cabe mencionar que la norma no cubre explícitamente el área de acciones legales y/o disciplinarias por el tratamiento inaceptable de la evidencia digital. Específicamente, declara que el cumplimiento de la ley y la reglamentación nacional aplicable debe garantizar su aplicación, y no anula las especificaciones jurisdiccionales del órgano rector de cualquier estado. Si bien la norma puede servir como guía práctica para los especialistas en evidencia digital durante las investigaciones, no profundiza en aspectos legales como la admisibilidad, el peso probatorio, la relevancia o las limitaciones legales que rigen el uso de la evidencia digital en los tribunales. No obstante, proporciona una referencia que permite compartir evidencia digital entre jurisdicciones, por lo que los procesos descritos pueden modificarse de acuerdo con la normativa de cada país.

Uno de los elementos más críticos en el manejo de la evidencia digital es la Cadena de Custodia (CoC), que define los requisitos marco mínimos que se deben seguir para confiar de manera adecuada y válida en la evidencia. Estos abarcan la asignación de un identificador de objeto único para cada pieza de evidencia, la descripción exacta de quién, cuándo y dónde se accede a la evidencia, y el registro estricto del movimiento de la evidencia de un lugar a otro, y todas las operaciones involucradas. Es muy recomendable que todas las alteraciones a la evidencia digital se documenten cuidadosamente, incluyendo el nombre de la persona que realiza el cambio y una explicación concisa y racional del cambio que se ha implementado, preservando la trazabilidad e integridad de la evidencia durante todo el proceso.

La obtención y manejo de pruebas digitales representan un pilar fundamental en el desarrollo de investigaciones forenses y judiciales en la actualidad, dado el auge de la tecnología y su impacto en la comisión de delitos. La transformación digital ha expandido la forma en que los crímenes son

cometidos, documentados y rastreados, haciendo que las pruebas digitales se conviertan en elementos esenciales en los procesos judiciales modernos. Para que estas evidencias cumplan con su propósito, es indispensable aplicar buenas prácticas que aseguren su validez y admisibilidad en los tribunales. La credibilidad de una prueba digital no depende únicamente de su contenido, sino de un tratamiento exhaustivo y riguroso que garantice su integridad y autenticidad en todas las etapas del proceso de recolección y análisis.

La prueba electrónica en el derecho comparado

Colombia

En Colombia, la introducción de la prueba digital en los procesos judiciales ha ido cambiando paulatinamente, debido al desarrollo de las TIC y a un contexto normativo más amplio. Desde las primeras codificaciones del Código de Procedimiento Civil, hasta definiciones más instrumentalizadas en la legislación posterior, la prueba digital ha adquirido legitimidad como elementos admisibles para sustentar hechos y resoluciones judiciales. La Ley 527 de 1999 marcó un paso decisivo al definir los mensajes de datos, es decir, toda información generada, transmitida, recibida o almacenada electrónicamente, creando así las bases para su reconocimiento formal como prueba. Esta normatividad allanó el camino para que los correos electrónicos, los mensajes instantáneos y otros registros digitales fueran admitidos en los procesos judiciales.

Posteriormente el Código General del Proceso, aprobado mediante la Ley 1564 de 2012, unificó la regulación de la prueba electrónica. Este cuerpo normativo establece en sus artículos 269 y 272 las condiciones bajo las cuales las partes pueden impugnar estos medios de prueba, exigiendo la acreditación de su autenticidad mediante informes periciales o mecanismos técnicos fehacientes. Además, el artículo 247 contempla la valoración de esta prueba por parte del juez, quien deberá evaluar tanto su contenido como las circunstancias de su obtención. En la práctica, tales artículos permiten, por ejemplo, hacer uso de una captura de pantalla de una conversación de WhatsApp, de contenidos en redes sociales y del propio correo electrónico, como prueba, siempre que se pueda rastrear su integridad y su origen.

Otro factor que ha contribuido al auge del uso de la prueba electrónica en el país ha sido el desarrollo de la jurisprudencia. La Corte Constitucional en 2020 adoptó la definición de prueba electrónica que fue propuesta por Federico Bueno de Matta, quien dice que la prueba electrónica consta de un componente material y un componente informativo. El primero es lo que generalmente

se conoce como hardware, es decir, la máquina en la que se produce o almacena la prueba, como una computadora o un teléfono celular. El segundo se refiere al software (metadatos y archivos electrónicos discretos que, a través de interfaces informáticas, comparten información sobre la naturaleza y características reales de la prueba). Esta definición amplía el rango en el que la prueba electrónica ha sido definida por el GARP más allá de aquellos formatos fácilmente identificables, y además se integra con algunas especificaciones técnicas para garantizar la confiabilidad y precisión.

La revolución jurídica despegó en 2020 a raíz de la crisis sanitaria de la enfermedad por coronavirus-19, que no solo abrió las posibilidades de la tecnología en el sistema jurídico, sino que lo revolucionó. En este contexto, y mediante el Decreto Legislativo 806 de 2020, se establecieron reglas específicas sobre la digitalización del acceso a la justicia en lo que respecta a la presentación de pruebas, en forma "electrónica". La implementación de esta norma vino de la mano no solo de permitir la continuidad de los procesos durante la crisis, sino también de fortalecer la prueba digital como una de las líneas centrales de trabajo del sistema jurídico colombiano, garantizando un mejor desempeño y acceso al trabajo.

El manejo de la prueba electrónica en Colombia está regulado por una serie de normas. Además de la Ley 527 de 1999 y el Código General del Procedimiento, el Código de Procedimiento Penal de 2004 confirma su papel en la etapa de investigación penal y el proceso penal. Todas estas leyes y el desarrollo de la jurisprudencia no sólo permiten el uso de este tipo de pruebas, sino que exigen procedimientos rigurosos para autentificarlas y probarlas, en un esfuerzo por mitigar el desafío de hacer valer tales derechos fundamentales en una sociedad digitalizada.

Se plantea los mensajes de datos en el artículo 424, párrafo 7, como una prueba, esta contribución responde a la creciente demanda de avanzar hacia la incorporación del pasado del sistema de justicia penal, así como de la tecnología de comunicación y registro de información. A la luz de esta regulación, los mensajes de datos se consideran prueba documental, lo que significa que su manejo y evaluación se relaciona con los documentos físicos de manera similar a un documento en papel. Este método trata de demostrar que los medios electrónicos no son menos válidos y confiables que sus contrapartes en soporte físico siempre que cumplan con los siguientes criterios (Yepes et al., 2022).

Para que un mensaje de datos sea recibido y analizado con valor probatorio, debe ser proporcionado de manera que conserve tanto la presentación como el contenido del mensaje. Esto implica que el

archivo o documento electrónico no debe incluir modificaciones o contaminaciones que puedan afectar la autenticidad. Además, su texto debe ser específico y suficientemente bien descrito para permitir al juez reunir mejor las pruebas concluyentes para construir una imagen fiel del caso. En otras palabras, no es suficiente que el mensaje de datos realmente exista; debe ser suficientemente completo o íntegro y suficientemente neutral o libre de ambigüedad para permitir un análisis minucioso y separado a los efectos del proceso penal.

Por esa razón, la prueba electrónica plantea interrogantes en torno a la autenticidad, la privacidad individual y de las partes y la justicia procesal, respectivamente. Dicha prueba debe ser utilizada y reclamada con prudencia por los jueces y los abogados con asistencia técnica, y por lo tanto de acuerdo con los principios del debido proceso y la equidad. Por tanto, la aceptación de la prueba digital en el proceso judicial, así como su utilización, no es sólo una aplicación de estatus, la provisión de una perspectiva correspondiente a las exigencias del mundo contemporáneo, sino también el deseo de crear un mejor sistema de justicia en el contexto moderno.

España

Una distinción importante entre el proceso penal como campo y sus principios radica en la estructuración y valoración de la prueba, que se justifica sustancialmente como tal. En primer lugar, el derecho a guardar silencio, encontramos el principio de presunción de inocencia que es la ley procesal que rige el proceso penal. Este principio trae la noción fáctica de que el acusado debe ser considerado culpable si el acusador no puede probar su culpabilidad más allá de una duda razonable, con la consiguiente absolución. El principio de inocencia desempeña un papel importante en la protección del individuo frente a la acusación perjuriosa, además de transferir la carga de la prueba del acusador. Por esa razón, es un componente clave de la decisión en el proceso y en el proceso de generación y preparación de la sentencia.

Existe otro principio que está estrechamente vinculado a esta cuestión, a saber, el principio de inmunidad del acusado frente a las confesiones, que garantiza el derecho del acusado a permanecer en silencio y a no implicarse durante el proceso penal. Esta idea está estrechamente relacionada con la perspectiva de la prueba de oficio, es decir, la capacidad del juez de hacer algo para garantizar el proceso de investigación de la verdad de las cosas. Se contrasta con los procesos dispositivos en los que las partes son las principales responsables de la producción y gestión de la prueba.

La posición primordial que se otorga al Poder Judicial en los procesos penales y el juicio se basa en los numerosos esquemas elaborados para proteger los derechos constitucionales y legales del acusado y, a su vez, garantizar la imparcialidad y la transparencia del proceso. Además, la valoración de la prueba en el ámbito penal se lleva a cabo con base en el principio de libre apreciación o valoración en conciencia. En la medida en que el juez, en lugar de limitarse a lo convencional, tiene que forjar su elección razonada por sí solo, esta es una buena ocasión para enfatizar el punto de que la elección en el análisis del caso debe basarse únicamente en la razón y la racionalidad.

Tal y como se recoge en el artículo 741 de la Ley de Enjuiciamiento Criminal, la referida libertad de valoración se reconoce también en la jurisprudencia del Tribunal Superior de Justicia, expresada en la Sentencia 31/1981, de 28.07, donde la valoración debe realizarse sobre la base de la interpretación regular y lógica de la prueba que se practica. Se entiende por material electrónico de prueba todo material con posibilidad fundamental de ser aportado a un tribunal para su tramitación como prueba electrónica o en soporte. Este tipo de prueba se califica como fundamental para la investigación de los delitos en la era de la cuarta revolución industrial, por ser cualquier práctica, registro, acta, dato o información captada en soporte electrónico que pueda ser pertinente para el establecimiento de hechos en el curso de un proceso penal.

En este sentido, la prueba electrónica puede ser de muy diversa índole, según la naturaleza en que se haya incorporado al proceso y el carácter legal de su introducción (como prueba documental, pericial o testimonial, según el caso) y según el soporte en que se presente y el carácter de su introducción en el momento de su presentación. Sin embargo, es importante destacar que el modo principal de generación de evidencia se deriva de la naturaleza misma de estos medios tecnológicos, lo que enfatiza el papel de la tecnología en la producción de evidencia en un mundo moderno y postindustrial.

En consecuencia, la prueba electrónica también presenta grandes dificultades para la posible afectación de derechos fundamentales. Algunas actuaciones gubernamentales pueden realizarse por vía electrónica, siempre que se mantengan dentro de los límites constitucionalmente permisibles para garantizar el respeto de los derechos individuales. El registro penal que incluye la incautación de dispositivos informáticos o la interceptación de telecomunicaciones, que se utiliza con frecuencia en la obtención de pruebas electrónicas, afecta a la esfera de la intimidad personal que la Constitución Española define en el artículo 18.1. Cualquier intromisión en este derecho debe,

en principio, ser autorizada por una decisión judicial o por el consentimiento de la persona afectada, salvo en casos de necesidad que justifiquen la actuación policial, siempre que se cumpla el necesario test de proporcionalidad que se ajuste a la sentencia del Tribunal Supremo 115/2913.

Además, estas acciones también pueden afectar a otras libertades de derechos humanos, por ejemplo, la libertad de secreto de las comunicaciones (artículo 18.3 CE) y la libertad de inviolabilidad del domicilio (artículo 18.2 CE), especialmente si los dispositivos utilizados están situados en el recinto más protegido por la ley: el domicilio particular. De manera similar, en el campo de la protección de datos personales, la autodeterminación informativa, reconocida en el artículo 18.4 CE, cobra un primer plano, ya que la información contenida en los dispositivos electrónicos es sensible y su procesamiento cumple fines legales, permisibles y razonables. En consecuencia, la regulación de la relación entre la efectividad de la investigación y la protección de los derechos constitucionales clave sigue siendo una cuestión aguda de la práctica del proceso penal moderno.

Metodología

La investigación adoptó un enfoque cualitativo, orientado a comprender y analizar de manera profunda la regulación y aplicación de la prueba digital en los procesos penales en Ecuador. Este enfoque permitió interpretar la normativa vigente, identificar sus deficiencias y proponer mejoras basadas en el análisis de textos legales y doctrinarios. El estudio se desarrolló a un nivel descriptivo, ya que se enfocó en detallar y caracterizar el tratamiento jurídico de la prueba digital en el Código Orgánico Integral Penal (COIP) de Ecuador, además de describir los procedimientos actuales para la gestión de evidencia digital y compararlos con los estándares internacionales.

Para abordar los objetivos planteados, se emplearon los métodos comparativos, inductivo-deductivo y dogmático jurídico. El método comparativo se utilizó para contrastar la normativa ecuatoriana sobre la prueba digital con los estándares internacionales, especialmente con la norma ISO 27002:2013, lo que permitió identificar brechas y oportunidades de mejora en la legislación nacional. Por su parte, el método inductivo facilitó la recolección y el análisis de información específica sobre la aplicación de la prueba digital en el contexto ecuatoriano, mientras que el método deductivo posibilitó interpretar y aplicar principios generales del derecho y estándares internacionales para proponer soluciones normativas. El método dogmático jurídico, en cambio, se centró en el análisis teórico y sistemático de las normas legales, doctrinas y jurisprudencia

relacionadas con la prueba digital en Ecuador, evaluando la coherencia y suficiencia de la normativa vigente, identificando vacíos legales y proponiendo ajustes pertinentes.

La técnica utilizada para la recopilación de información fue la revisión bibliográfica, que consistió en el análisis de fuentes documentales relevantes como libros, artículos científicos, legislación nacional e internacional, doctrina y jurisprudencia vinculada a la prueba digital. Esta técnica proporcionó el sustento teórico y legal necesario para comprender el estado actual de la normativa ecuatoriana y sus desafíos. El instrumento de recolección empleado fue el fichaje, mediante el cual se organizó y sistematizó la información recopilada. Las fichas bibliográficas permitieron registrar de manera ordenada los datos extraídos de las fuentes consultadas, lo que facilitó un análisis crítico y comparativo. Se elaboraron fichas textuales, de resumen y de comentario, lo que posibilitó una interpretación integral de los textos legales y doctrinarios revisados.

El procedimiento de investigación incluyó la selección de fuentes relevantes, la elaboración de fichas bibliográficas, el análisis comparativo entre la normativa nacional y los estándares internacionales, la interpretación jurídica a través del método dogmático y la síntesis de resultados. Esto permitió formular conclusiones y recomendaciones orientadas a mejorar la regulación y aplicación de la prueba digital en Ecuador.

Resultados

Las normas que regulan la prueba digital en el contexto del ordenamiento jurídico ecuatoriano, contenidas principalmente en el Código Orgánico General de Procesos, constituyen un buen esfuerzo de su ordenamiento jurídico por integrar la aplicación de sus procedimientos a los nuevos cambios y desafíos que plantea el actual mundo altamente informatizado. Este órgano gubernamental crea normas especiales para la admisión y consideración de la prueba digital, que se está convirtiendo en la norma en los procesos judiciales a medida que aparecen nuevas tecnologías de comunicación y distribución de información. La prueba electrónica en los procesos civiles y penales en el Ecuador se expresa en un conjunto de reglas para determinar la relación, la fiabilidad y el respeto al debido proceso, de acuerdo con la Constitución del Ecuador que garantiza el derecho de defensa y el acceso a la justicia.

El COGEP establece además condiciones precisas de admisibilidad de la prueba digital, pues como se establece, ninguna prueba, incluida la digital, puede ser admitida sin ser pertinente y adecuada al caso presentado. Esto significa que el juez tiene que garantizar que la prueba digital sea admisible

al caso en las circunstancias fácticas y que, en ausencia de buenas razones para hacerlo, la prueba no esté contaminada por datos irrelevantes o intromisión en los derechos privados de las partes. Sin embargo, una de las condiciones previas más fundamentales para la decisión sobre su admisibilidad es su legalidad, es decir, que se hayan tomado en cuenta las normas legales sobre la protección de la privacidad y los datos personales. Cualquier medio de violación de las leyes estadounidenses mediante la obtención de referencias virtuales, por ejemplo, correo electrónico, redes sociales, etc., tiene consecuencias negativas en la admisibilidad de dicha prueba, restablecerá la responsabilidad legal de la parte al presentarla como legalmente vinculante para restablecer el derecho de las personas infringidas.

En la jurisprudencia ecuatoriana, la relevancia del uso de la prueba digital está directamente asociada al derecho de defensa, derecho constitucional que garantiza a los diferentes actores del proceso todos los recursos necesarios para defender sus derechos e intereses. En el contexto de la prueba digital, esto significa que las partes tienen permitido presentar e impugnar este tipo de prueba, siempre y cuando sea auténtica y no haya sido manipulada. No es difícil ver, ya que por la naturaleza misma de la prueba digital los hechos pueden ser fácilmente manipulados y distorsionados, que la imparcialidad también se verá afectada por esto. En consecuencia, la legislación establece que la prueba digital requiere pasar por un proceso de verificación para demostrar que la prueba ha sido preservada en el estado en que fue creada y no ha sido manipulada de manera que la vuelva inadmisible.

El COGEP también subraya que la prueba digital efectivamente exhibida tiene que ser de fácil comprensión y fácil aceptación por el tribunal, dos directrices que tienen como objetivo permitir a los jueces y abogados comprender estos aspectos, ya que en muchos casos no tienen los conocimientos técnicos suficientes para operar tales sistemas. La comprensibilidad obligatoria y suficiente significa que los documentos, imágenes, archivos de audio y video y otras pruebas electrónicas relacionadas deben presentarse en una presentación ordenada y fácilmente comprensible de sus elementos. Sin embargo, no es sorprendente que también se pueda hablar de la necesidad de verificabilidad, como permitir garantizar que la prueba pueda ser examinada para verificar su fuente, su autor y el contenido mismo. Con este requisito, se garantiza que, después de la creación de cualquier pieza de prueba digital, exista un seguimiento a través del cual se puedan rastrear los procesos de generación, almacenamiento y transmisión y que se asegure una relación entre la prueba presentada y los hechos considerados en el proceso.

Uno de los requisitos más importantes en la evaluación de la validez de la prueba digital es la capacidad de compararla con las herramientas utilizadas en su creación o adquisición. Esto también significa que muchas veces se deben proporcionar los originales de los dispositivos, o de los sistemas que produjeron la evidencia digital, para autenticarlos. En concreto, cuando se proporciona una anotación, no sólo necesitamos una captura de pantalla de un mensaje de texto o de un correo electrónico, sino también una prueba del dispositivo que utilizamos para entregar esa evidencia (para evitar dudas sobre la validez de la evidencia) y que no haya sido modificado. Esta precaución está dirigida a los probables intentos que son generalizados en el entorno digital por el grado de manipulación de documentos digitales que permite, aunque riesgosos en lo que respecta a la admisibilidad judicial de los documentos.

Sin embargo, la cantidad de desafíos que Ecuador necesita abordar para implementar adecuadamente el COGEP en relación con la evidencia digital aún es sustancial, incluso después de estos cambios legales regionales y nacionales. Uno de ellos se refiere al problema de la falta de continuidad en la formación de los operadores de justicia, incluidos jueces y abogados, que necesitan desarrollar habilidades especiales para evaluar la evidencia digital en función de su autenticidad, reproducibilidad y relevancia. Observando la naturaleza de la primera pregunta de investigación y la complejidad y variabilidad de la producción de evidencia digital, derivada de la rápida evolución de la tecnología y la gran cantidad de dispositivos y aplicaciones, se ha observado que el desafío de mantener actualizado el conocimiento y adoptar nuevas técnicas de análisis no es fácil de abordar, sin proporcionar un esquema de capacitación continua ad hoc para el campo.

La falta de reglas claramente definidas para la presentación y extracción de evidencia digital es la segunda falla de los tribunales ecuatorianos. La falta de ciertos estándares para la admisibilidad y autenticación de este tipo de evidencia plantea el riesgo de falta de certeza en la evaluación de la regulación por parte de varios tribunales y podría afectar la seguridad jurídica. La elaboración y definición de procedimientos que sean confiables en todas las etapas, desde la recolección de evidencia, incluidos todos sus tipos, hasta su intercambio, está bien justificada para garantizar que todos estos elementos puedan emparejarse y, a su vez, garantizar que el proceso de manipulación de la evidencia no ocurra en esta área, y que garantizará entonces una mayor transparencia del procedimiento, evitando cualquier ilegalidad.

Existen en el mundo numerosos instrumentos y tratados internacionales que tienen como objetivo definir estándares para el almacenamiento, recolección y gestión de evidencia digital, entre ellos el

Convenio de Budapest, un acuerdo internacional destinado a fomentar la cooperación y establecer estándares para la recolección y salvaguarda de evidencia digital y la lucha contra los delitos informáticos. Debido a que Ecuador aún no se ha adherido a estos estándares internacionales, estos presentan desventajas en el contexto de los delitos digitales, que al ser mayoritariamente transnacionales, requieren tanto de financiamiento como de cooperación, y de la aplicación de una legislación similar para lograr un buen efecto disuasorio. A diferencia de otros Estados de la región que ya se han convertido en partes contratantes del Convenio de Budapest, Ecuador es un Estado que presenta una particularidad, pues actualmente se encuentra en un proceso de actualización de su legislación para adquirir una calidad efectiva y segura a la hora de evaluar la evidencia digital similar a otras jurisdicciones.

Alineado con los principios generales, la norma internacional exige la cadena de custodia, la autenticidad y la integridad de las pruebas digitales, medidas que corresponden aproximadamente a las disposiciones de la COGEP pero que pueden implementarse de manera diferente según las jurisdicciones. La cadena de custodia, que asegura que las evidencias digitales no sean manipuladas en cualquier momento de su recopilación o traslado, es un principio básico que garantiza la integridad y el escrutinio científico de la evidencia. La autenticidad y la integridad por otro lado permite verificar que la prueba digital en cuestión es efectivamente la prueba correspondiente a los hechos que se quieren demostrar para evitar un montaje que contagie al juicio.

Por último, en comparación con otros países de la región que han ratificado el Convenio de Budapest y tienen sólidas regulaciones en materia digital en general y en pruebas digitales en particular, Ecuador se encuentra en un ligero retraso normativo que podría impactar no sólo la calibración del sistema judicial, sino también los casos en que puedan existir delincuentes digitales o cualquier otra situación que Este rezago evidencia la necesidad que tiene el país de modernizar su legislación en esta materia y esforzarse en lograr la implementación de estándares internacionales que hagan crecer la seguridad y confiabilidad de los datos digitales asegurando que el sistema judicial del país se adapte a las condiciones de la era digital y la promoción de acceso a la justicia en el país.

Propuesta

El sistema judicial ecuatoriano se encuentra en un punto crítico en cuanto a la integración efectiva de la prueba digital en los procesos penales. Esta necesidad ha sido impulsada por el crecimiento

de los delitos informáticos y la relevancia cada vez mayor de las tecnologías digitales en las conductas delictivas tradicionales. Sin embargo, existen limitaciones sustanciales en el marco normativo, las capacidades técnicas de los operadores de justicia y la infraestructura tecnológica disponible, lo que compromete la admisibilidad, validez y efectividad de las pruebas digitales. Para abordar esta problemática, es fundamental llevar a cabo una serie de reformas normativas y estructurales, así como implementar buenas prácticas que garanticen la incorporación efectiva de estas evidencias en el sistema judicial del país.

En primer lugar, es necesario analizar las deficiencias normativas. Aunque el Código Orgánico Integral Penal (COIP) reconoce la validez de la prueba digital, no proporciona una regulación específica que establezca protocolos claros sobre su autenticación, cadena de custodia y presentación en juicio. Esto crea vacíos legales que dificultan su admisibilidad, ya que las partes procesales pueden cuestionar la fiabilidad y la integridad de la evidencia presentada. Además, la ausencia de lineamientos estandarizados permite interpretaciones divergentes entre los operadores judiciales, lo que afecta la uniformidad en los fallos y genera incertidumbre jurídica. Es esencial que el sistema judicial ecuatoriano desarrolle normativas específicas inspiradas en estándares internacionales como las normas ISO/IEC 27037, 27041 y 27042, las cuales ofrecen directrices detalladas para la gestión, análisis y validación de pruebas digitales. Estas normativas pueden ser adaptadas al contexto ecuatoriano para garantizar su efectividad en la lucha contra delitos complejos.

La cadena de custodia es otro aspecto crítico que requiere atención urgente. Según el COIP, la cadena de custodia debe garantizar la autenticidad e integridad de las pruebas desde su recolección hasta su presentación en juicio. Sin embargo, en la práctica, muchas evidencias digitales no son manejadas conforme a protocolos técnicos rigurosos, lo que abre la posibilidad de alteraciones o manipulaciones que podrían invalidarlas. Por ejemplo, en casos emblemáticos como los de corrupción en Petroecuador o el caso "Sobornos 2012-2016", la falta de protocolos claros para preservar la integridad de los correos electrónicos y registros electrónicos utilizados como evidencia digital fue un tema de debate. Esto evidencia la necesidad de implementar procedimientos estandarizados que documenten de manera rigurosa cada etapa del manejo de la evidencia digital, desde su extracción hasta su almacenamiento y análisis.

Además de las deficiencias normativas y técnicas, se observa una carencia significativa de capacitación entre los operadores judiciales. Los jueces, fiscales y abogados suelen carecer de

formación especializada en informática forense y manejo de pruebas digitales, lo que limita su capacidad para evaluar adecuadamente la autenticidad, relevancia y validez de estas evidencias. Este problema se agrava en un contexto donde las tecnologías digitales evolucionan rápidamente, presentando nuevos desafíos en términos de seguridad y análisis. La implementación de programas de capacitación continua en tecnología forense, legislación sobre delitos digitales y normas internacionales de manejo de evidencia es esencial para fortalecer las competencias de los operadores de justicia y garantizar un uso adecuado de las pruebas digitales en los procesos penales.

En el ámbito de infraestructura tecnológica, el sistema judicial ecuatoriano enfrenta limitaciones que obstaculizan el manejo eficaz de las pruebas digitales. La falta de herramientas modernas para recolectar, analizar y almacenar evidencia digital dificulta su utilización en los tribunales. Es fundamental que el Estado invierta en la adquisición de software y hardware especializados, así como en la creación de laboratorios de informática forense que operen bajo estándares internacionales. Estas instalaciones permitirían realizar análisis técnicos rigurosos que garanticen la integridad de la evidencia y faciliten su admisión en los procesos judiciales.

La creación de unidades especializadas dentro del sistema judicial y las fiscalías es otra medida necesaria para fortalecer el manejo de las pruebas digitales. Estas unidades, integradas por expertos en informática forense, podrían desempeñar un rol clave en la recolección, análisis y presentación de evidencias digitales, así como en la asesoría técnica a los operadores de justicia en casos complejos. Su creación no solo mejoraría la calidad del manejo de pruebas digitales, sino que también promovería la transparencia y la confianza en el sistema judicial.

En el ámbito internacional, la adhesión de Ecuador al Convenio de Budapest sobre ciberdelincuencia sería un paso estratégico para mejorar la cooperación internacional en la investigación y el enjuiciamiento de delitos cibernéticos. Este convenio establece un marco común para la recolección y manejo de pruebas digitales, así como para la colaboración entre países en la lucha contra delitos transnacionales. Su implementación permitiría a Ecuador beneficiarse de buenas prácticas internacionales y fortalecer su capacidad para enfrentar los desafíos que plantea la evidencia digital en un mundo globalizado.

Por último, la promoción de buenas prácticas en el manejo de pruebas digitales es fundamental para garantizar su validez y admisibilidad en los tribunales. Esto incluye la implementación de protocolos claros para la recolección y preservación de evidencias, el uso de tecnologías avanzadas para el análisis forense y la creación de sistemas de certificación para peritos especializados. Estas

medidas contribuirían a mejorar la calidad y la fiabilidad de las pruebas digitales, asegurando que cumplan con los estándares de autenticidad, integridad y reproducibilidad necesarios para su admisión en juicio.

Conclusiones

La prueba digital ha puesto en escena como una cuestión esencial en la configuración del nuevo derecho penal del siglo XXI, se destaca en el ambiente de los delitos informáticos, en donde la acción delictual ocurre y siempre deja alguna huella en el ciberespacio. Esta clase de evidencia no solo testimonia un desarrollo tecnológico de cómo administrar Justicia, sino que, al actualizarse, se ha convertido en una herramienta con un componente ético práctico para asegurar que los procesos y trámites judiciales sean relevantes y correctos. Su importancia se basa en la característica de su capacidad de ofrecer datos concretos, accesibles y de alta precisión los cuales son valiosos en el desenlace de casos difíciles, donde las evidencias ordinarias no son adecuadas o no están disponibles.

Pero al mismo tiempo, se encuentran en esta investigación algunos riesgos que se asocian con su aplicación en el ambiente del derecho en Ecuador. Un desafío relacionado es el inexiste de una normative adecuada que permita regular de forma efectiva la recolección, custodia, análisis y presentación de esta evidencia en el marco judicial. Los vicios que presenta la normativa actual hacen imposible asegurar la autenticidad e integridad de la prueba digital y como tal su credibilidad y validez en los juzgados. No solo estas carencias restringen al sistema de justicia para no procesar delitos relativo a tecnologías modernas, sino que también crea posibilidad de cuestionamientos y nulidades en los casos judiciales y produce inseguridad jurídica. Por lo tanto, surge la realidad y/o especificidad de llevar adelante reformas legales que permitan adecuar la normativa nacional con las normativas internacionales más vanguardistas y con las mejores prácticas a nivel internacional en torno a los temas referidos probidad digital.

La formación de los actores judiciales son otro de los aspectos esenciales para enfrentar esta problemática. Por un lado, la comprensión adecuada de la prueba digital necesita conocimiento técnico en campos como la forense y tecnologías de información de cuyo entramado tradicional de jueces, fiscales y abogados. Por falta de profesionalidad, uno puede volver a los datos equivocado o hasta descartar pruebas importantes en los procesos legales. Así que resulta esencial diseñar y poner en práctica cursos de capacitación que preparen a los operadores de justicia para que puedan

ejercer las habilidades requeridas para manejar, analizar e interpretar la evidencia digital con eficiencia. Así, se lograrían mayor trasparencia y confianza en el sistema judicial, en un mundo que es tan digital y va a requerir una justicia eficiente para la solución de conflictos.

Por lo tanto, este estudio aporta al saber de la especialidad del derecho penal al ofrecer un diagnóstico acerca de la realidad de la prueba digital en el Ecuador y recomendaciones para su desarrollo. Cuando se investiga las consecuencias de la revolución tecnológica en el campo legal, no solo se arrojan luces a las falencias que prevalecen, sino también propuestas a cómo abordar dichos desafíos. Este enfoque integral configura el marco que futuros estudios y cambios diseñarán un sistema de justicia capaz de responder eficaz a las exigencias del clima digital. Al mismo tiempo, frecuentemente sirve como base para otros países de la región, los cuales también experimentan semejantes problemas, y así, ayuda al desarrollo discusión más general de la temática de modernización del derecho penal en el contexto del mundo.

Por lo tanto, los objetivos establecidos al inicio de esta investigación se han logrado con cierta medida de satisfacción. Entre ellos, la determinación de las lagunas de la actual reglamentación, la evaluación crítica de la función de la prueba digital en los procesos judiciales y las alternativas para su mejoramiento. Tales respuestas además de fortalecer el campo de conocimiento son igualmente convenientes para su aplicabilidad a partir de las recomendaciones que proveen soluciones realistas para mejorar el acceso a la justicia en el Ecuador. Por ende, el estudio no sólo responde con la finalidad, sino que también posicionar al estudio como un banco de soluciones para producir cambio estructural en el sistema judicial egresando al requisito que una sociedad cada vez más guiada por le tecnología digital requiere.

En tal sentido, es fundamental que el sistema normativo de Ecuador, cuya actualización se encuentra en proceso sea modificado y ajustado a las innovaciones tecnológicas y a los modelos normativos internacionales en materia de prueba digital. Lo anterior implica la elaboración de leyes especiales que regulen la recopilación, conservación, análisis y presentación del material digital y garantizar su legalidad, integridad y certeza. Asimismo, estas reformas deben incluir criterios técnicos que permitan la definición de protocolos, tales como, las cadenas de custodia digital sólidas y la metodología del análisis forense bien establecido a nivel mundial. Esta adecuación normativa mejoraría notoriamente la seguridad jurídica y eliminaría cualquier posibilidad de exclusión o impugnación de pruebas en los órganos jurisdiccionales.

Por lo tanto, se sugiere implementar un programa nacional de capacitación permanente dirigido a jueces, fiscales, abogados y otros actores de la justicia con especial aplicación técnica y jurídica en la prueba digital. Esta formación supuestamente debe diseñar módulos específicos en relación a la informática forense, procesos de adquisición de datos tecnológicos y los protocolos locales e internacionales correspondiente. Es por ello que la capacitación debe ser diseñada de tal manera que permita que los actores del sistema judicial no solo conozcan los aspectos técnicos de la evidencia digital, sino también las implicancias legales con el propósito de que pueda haber una debida evaluación durante los distintos procesos judicial.

Asimismo, se plantea la formación de estructuras especiales dentro del sistema judicial y las fiscalías estipuladas por especialistas en tecnologías de la información e informática forense. Estas unidades serían técnicamente acreditas para apoyar en la recopilación y en el análisis de la evidencia digital además para apoyar a los operadores de justicia en casos difíciles con relación a delitos digitales o pruebas tecnológicas complejos. Esta especialización institucional ayudaría a asegurar un mejor y más adecuado control de las pruebas digitales allegados y rendidos asegurando un mejor control y confusión al sistema judicial.

El otro factor clave consiste en inversión en maquinaria tecnológica para equiparar el sistema judicial con recursos eficaces para recolección y capacitación digital con una mayor precisión. Este se produce a través de la compra de software y la adquisición de equipos especializados con la capacidad de llevar sistemas de manejo de información electrónica que faciliten los trámites legales de forma segura. Lo que se hace necesario es utilizar la tecnología no solo como medio y fin, sino como una herramienta que permita garantizar que dicha prueba digital sea sometida a los mejores niveles técnicos y éticos posibles.

Por ello, se debe propiciar la colaboración internacional en temas de regulación y gestión de la prueba digital. Inscribiendo acuerdos e integración con organismos internacionales junto con países más experimentados en este campo ayudaría al Ecuador en obtener buenas prácticas y mejores tecnologías. Además, el activo compromiso en las conferencias internacionales sobre cibercrimen y antecedentes digitales brindaría al país mayores opciones para abordar los desafíos relacionados con la integración a la economía global y los delitos informáticos.

Referencias

1. Araujo, F. (2010). La prueba y su incorporación al proceso en el juicio penal. Universidad de Cuenca. http://dspace.ucuenca.edu.ec/bitstream/123456789/2933/1/td4311.pdf
2. Asamblea Nacional de Ecuador. (2023). Código Orgánico Integral Penal. Registro Oficial Suplemento 180, 2014-02-10. https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf
3. Asamblea Nacional del Ecuador. (2015). Código Orgánico General de Procesos. Registro Oficial Suplemento 506 de 22-may.-2015. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Orgánico-General-de-Procesos.pdf
4. Banegas, D., & Andrade, D. (2022). Análisis Forense en Dispositivos Móviles Android para Casos de Ciberextorsión, Revisión Sistemática de Literatura. MQRInvestigar , 8(3), 4076-4097. https://doi.org/10.56048/mqr20225.8.3.2024.4076-4097
5. Bielli, G. (2019). Prueba electronica: incorporacion, admision y valoracion de capturas de pantalla en el proceso de familia. Argentina: Pensamiento civil.
6. Borges, R. (2018). La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea. Iuris Tantum(25), 536-549. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100018
7. Bujosa, L., & Toro, M. B. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. Revista Brasileira de Direito Processual Penal, 7(2), 1347-1384. https://doi.org/10.22197/rbdpp.v7i2.482
8. Bustamante, M. (2010). La relación del estándar de prueba de la duda razonable y la presunción de inocencia desde el garantismo procesal en el Proceso Penal Colombiano. Opinión Jurídica, 9(17), 71-91. https://www.redalyc.org/pdf/945/94516348004.pdf
9. Cafferata, J. (2003). La prueba en el proceso penal con especial referencia a la ley 23.984 (Quinta edición). Depalma. https://aulavirtual4.unl.edu.ar/pluginfile.php/6886/mod_resource/content/1/La-prueba-en-el-Proc.-Penal.-Cafferata-Nores.pdf

10. Campoverde, L. (2013). El Principio de inocencia y la carga de la prueba en el proceso penal. Contribuciones a las Ciencias Sociales(20), En línea. https://www.eumed.net/rev/cccss/20/yst3.html
11. Carbone, C. (2016). Incorporacion de la prueba al juicio: prohibicion de introducción por lectura de prueba testimonial y material. Revista Académica Electrónica de la UNR, 9(17). http://hdl.handle.net/2133/6671
12. Consejo de Europa. (2001). Convenio de Budapest sobre la Ciberdelincuencia,. Serie de Tratados No. 185. https://rm.coe.int/1680081561
13. Consejo de Europa. (2023). Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. Diario Oficial de la Unión Europea L 63/28. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A22023A0228%2801%29
14. De Malta, B. (2014). Prueba electronica y proceso 2.0. España: Tirant lo blanch.
15. González, J. (2021). La prueba digital y la cadena de custodia. Anales de la Facultad de Derecho(38), 43-79. https://doi.org/10.25145/j.anfade.2021.38.03
16. López, Z. (2023). Validez Jurídica de la prueba digital en Guatemala. Revista Ciencia Multidisciplinaria CUNORI, 7(2), 203–214. https://doi.org/10.36314/cunori.v7i2.238
17. Magro, V. (2020). Casuística práctica de la prueba digital en el proceso civil y penal. Actualidad civil(1). https://dialnet.unirioja.es/servlet/articulo?codigo=7400340
18. Martínez, G. (2022). Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. Revista Electronica de Ciencia Penal y Criminologia, 24-23, 1-38. https://reunir.unir.net/handle/123456789/15287
19. Merino, J. (2024). Cadena de custodia: Valoración de prueba y tutela judicial efectiva en el procedimiento adversarial penal. Ciencia Digital, 8(2), 36-63. https://doi.org/10.33262/cienciadigital.v8i2.2966
20. Molina, C., Beltrán, L., & Contreras, O. (2021). LA PRUEBA ELECTRÓNICA Y DIGITAL. Aclaración de las diferencias jurídicas en Colombia. Institución Universitaria Politécnico Grancolombiano. https://alejandria.poligran.edu.co/bitstream/handle/10823/2147/La%20prueba%20Electronica%20y%20digital.pdf?sequence=2&isAllowed=y

21. Organización Internacional de Normalización. (2012). ISO/IEC 27037:2012. ISO. https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf
22. Organización Internacional de Normalización. (2015). ISO/IEC 27041:2015 Tecnologías de la información -tecnologías de la seguridad- directrices para asegurar la adecuación de métodos de investigación de incidentes. ISO. https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027041-2015.pdf
23. Organización Internacional de Normalización. (2015). ISO/IEC 27042:2015 Tecnologías de la información – tecnologías de seguridad – líneas directrices para el análisis e interpretación de evidencia digital. ISO. https://cdn.standards.iteh.ai/samples/44406/c986892bfdca440fa33c5eda1e57e23a/ISO-IEC-27042-2015.pdf
24. Organización Internacional de Normalización. (2015). ISO/IEC 27043:2015 Tecnologías de la información – tecnologías de la seguridad – principios de investigación numérica en los procesos. ISO. https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027043-2015.pdf
25. Pintado, A., & Ochoa, F. (2021). La obtención y validez de la prueba de audio y video, realizada por los agentes civiles de tránsito de la Ciudad de Cuenca, en las contravenciones de tránsito de primera clase, por transportar pasajeros sin tener el título habilitante. FIPCAEC (Edición 25), 6(3), 416-449. https://doi.org/10.23857/fipcaec.v5i14.176
26. Porras, P. (2023). La Incorporación de la Prueba Digital en el Proceso Penal Colombiano. Unilibre. https://repository.unilibre.edu.co/handle/10901/29366?locale-attribute=es
27. Quichimbo, M., Mereci, L., & Ramón, M. (2024). La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos. Dominio de las Ciencias, 10(3), 1126-1142. https://doi.org/10.23857/dc.v10i3.3972
28. Roatta, S., Casco, M., & Fogliatto, M. (2015). El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. XXI Congreso Argentino de Ciencias de Computación. Junin: UNLP. https://sedici.unlp.edu.ar/handle/10915/50586
29. Sarmiento, J., & Maldonado, L. (2024). DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR. MQRInvestigar, 8(3), 1753-1781. https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

30. Tixi, D., Iglesias, J., & Bonilla, C. (2022). Las audiencias telemáticas en materia penal y la correcta producción de los medios de prueba. Dilemas contemporáneos: educación, política y valores, 9(1). https://doi.org/10.46377/dilemas.v9i.3018
31. Vázquez, C. (2022). El panorama actual de la prueba digital en el contexto de la justicia electrónica en México en materia penal. Nueva época: Derecho y administración , 10(27), 43–71. https://doi.org/10.5281/zenodo.6539895
32. Yepes, M., Pérez, J., & Peinado, M. (2022). Aplicación de la prueba electrónica en el marco normativo colombiano. Novum Jus, 16(1), 253-277. https://doi.org/10.14718/NovumJus.2022.16.1.11