



N° 1, V. 10, ENERO-JUNIO 2024/ Revista Científica Multidisciplinaria/
ISSN: 2542-3037 <https://revistapt.edublogs.org/>



Deposito Legal: pp201502044688
ISSN: 2542-3037

Universidad Politécnica y Territorial
de Barinas José Félix Ribas
UPTB.JFR

EL MANEJO DE LA EVIDENCIA DIGITAL COMO PRUEBA EN EL PROCESO JUDICIAL PENAL VENEZOLANO

Dra. Juana Rosa Molina Brizuela, Estudiante de Doctorado en Derecho,
(juanamolbriz@gmail.com) (<https://orcid.org/0009-0003-8268-7415>)

RESUMEN

Este epítome corresponde a una investigación cuyo propósito fue analizar el manejo de la evidencia digital en el proceso judicial penal venezolano para establecer principios rectores del protocolo cadena de custodia, con una visión holística en la formación de eruditos afines con los avances y desafíos del derecho penal. Cimentada en la teoría los frutos del árbol envenenado, reflejada en la Biblia (Mateo 7: 17-20), con analogía en los aportes de Pereira (2014), una evidencia digital mal obtenida o asegurada implica una alta posibilidad de ser descartada como prueba, con la consecuente impunidad del hecho, pues dará lugar a sentencia fundamentada en lo que se conoce como doctrina del árbol envenenado. Se inserta en un paradigma postpositivista esgrimiendo un enfoque cualitativo encuadrado en una investigación de tipo documental con orientación hermenéutico aplicado al ámbito jurídico de nivel descriptivo e interpretativo, afirmado para dilucidar los hallazgos en las técnicas: categorización, triangulación y teorización. Definitivamente, es un desafío estudiar la prueba digital y protocolo de cadena de custodia en el contexto penal, pues tal aporte epistémico promueve la reflexión jurídica para esclarecer hechos delictivos y soslayar errores al determinar responsabilidad del inculcado.

Palabras Clave

Evidencia digital, prueba, proceso penal, judicial, jurídica.

Recibido: 2024-04-10 / Revisado: 2024-05-01 / Aceptado: 2024-05-25 / Publicado: 2024-06-25 / Pág. 485-504



THE HADLING OF DIGITAL EVIDENCE AS EVIDENCE IN THE VENEZUELAN CRIMINAL JUDICIAL PROCESS

Dra. Juana Rosa Molina Brizuela, Doctoral Student in Law,
(juanamolbriz@gmail.com) (<https://orcid.org/0009-0003-8268-7415>)

Abstract

This epitome corresponds to a research whose purpose was to analyze the management of digital evidence in the Venezuelan criminal judicial process to establish guiding principles of the chain of custody protocol, with a holistic vision in the training of scholars related to the advances and challenges of the criminal law. Based on the theory of the fruits of the poisoned tree, reflected in the Bible (Matthew 7: 17-20), with analogy in the contributions of Pereira (2014), poorly obtained or secured digital evidence implies a high possibility of being discarded as evidence. , with the consequent impunity of the act, since it will lead to a sentence based on what is known as the poisoned tree doctrine. It is inserted in a postpositivist paradigm using a qualitative approach framed in a documentary-type investigation with a hermeneutic orientation applied to the legal field at a descriptive and interpretive level, affirmed to elucidate the findings in the techniques: categorization, triangulation and theorization. It is definitely a challenge to study digital evidence and chain of custody protocol in the criminal context, since such epistemic contribution promotes legal reflection to clarify criminal acts and avoid errors when determining responsibility of the accused.

Keywords

Digital evidence, evidence, criminal process, judicial, legal.

Received: 2024-04-10 / Revised: 2024-05-01/ Accepted: 2024-05-25/ Published: 2024-06-25 / Pages: 484-504



Introducción

En la era del conocimiento e innovación tecnológica, el sistema procesal penal debe aprovechar los avances disponibles para fortalecer la justicia mediante la inclusión de la ciencia forense en la investigación. Esta transformación es posible gracias a la reflexión y adaptación de los operarios, científicos forenses, y expertos en el manejo de evidencias o pruebas digitales. Las evidencias digitales son definidas por Sanchis (2018) como “todas aquellas pruebas, evidencias y hechos recogidos, producidos o almacenados a través de los medios informáticos y las nuevas tecnologías. Cualquier dato que pueda ser relacionado con un delito, la víctima o el autor” (p.1).

Desde este orden de ideas Cortés, Di Iorio y Lagos (2020), consideran que debemos adaptarnos a las nuevas tecnologías e innovaciones, es decir a las nuevas formas de interactuar en una sociedad cada vez más compleja. Sin embargo es relevante destacar que las redes sociales y la tecnología, ayudan tanto a los investigadores en la resolución de delitos como a los delincuentes en la comisión del hecho punible. Los delincuentes utilizan dispositivos digitales para cometer crímenes, mientras que los investigadores deben adaptarse continuamente a las nuevas tecnologías.

De la misma forma, expresa Martínez (2022), abordar la nueva era electrónica en la que vivimos hace que cada vez más tengamos que acudir a la prueba digital para acreditar el hecho delictivo, ya sea en delitos clásicos o cibernéticos. Al respecto la Universidad en Internet (UNIR, 2021), considera que la informática forense juega un papel fundamental en la investigación y persecución de los cibercriminales, pues su objetivo principal es la obtención de evidencias relativas a un crimen digital.

El sistema de justicia penal venezolano ha enfrentado una crisis debido al aumento y complejidad de la criminalidad. Las estrategias tradicionales han sido insuficientes, y es ineludible que el sistema adopte avances tecnológicos y nuevos protocolos para manejar la evidencia digital



adecuadamente. El “Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela” (2022), ofrece un marco para el manejo de la evidencia digital, orientando las acciones de todas las personas participantes en el proceso penal. Este protocolo busca asegurar del tratamiento adecuado de las evidencias en cada fase del proceso penal.

Este estudio sobre el manejo de la evidencia digital en Venezuela tiene como propósito analizar y desarrollar conocimientos en las nuevas tendencias del derecho penal, contribuyendo al debate y creando alternativas jurídicas que vinculen la academia con la sociedad. Tomando como punto de partida el bosquejo antes señalado la investigadora se plantea las siguientes incógnitas sobre el manejo de la evidencia digital en el proceso judicial penal venezolano, enfocándose en aspectos teóricos y prácticos:

- ¿Cuál es la visión teórica sobre el manejo de la evidencia digital como prueba en el contexto judicial venezolano?
- ¿Existe un corpus teórico ontológico de protocolo para manejar la evidencia digital en el sistema de justicia procesal venezolano?
- ¿Cuáles son los desafíos que enfrenta el sistema judicial penal venezolano en el manejo de la evidencia digital como prueba?
- ¿Cuáles son los principios que guían el manejo de evidencia digital como prueba en el proceso judicial penal venezolano?
- ¿Cómo interpretar la teoría ontológica del manejo de la evidencia digital como en el contexto judicial penal venezolano?, de las cuales surgen los siguientes propósitos de la Investigación.

Propósito General: Analizar el manejo de la evidencia digital como prueba en el proceso judicial penal venezolano y **Propósitos Específicos:** a) Estudiar la existencia y aplicación de un corpus teórico ontológico de protocolo para manejar la evidencia digital en el sistema de justicia penal venezolano; b) Delimitar los desafíos en el manejo de la evidencia digital en el proceso judicial penal venezolano; c) Develar los principios rectores



establecidos para el manejo de evidencia digital como prueba en el proceso judicial penal venezolano y d) Interpretar la teórica ontológica del manejo de la evidencia digital en el contexto judicial penal en Venezuela.

El estudio se basa en la teoría “los frutos del árbol envenenado” y se enmarca metodológicamente en un paradigma postpositivista con un enfoque cualitativo. Es una investigación de tipo documental con orientación hermenéutica, descriptiva e interpretativa, aplicado técnicas documentales y de análisis como categorización, triangulación y teorización para interpretar los hallazgos en al ámbito jurídico.

Materiales y métodos

La investigación se basa en la construcción del estado del arte, definido por Londoño, Maldonado y Calderón (2014), como “una revisión detallada y cuidadosa de los documentos que tratan sobre un tema específico”. (p.6). Este proceso es esencial para entender el tratamiento, avance y tendencias en el manejo de la evidencia digital en el contexto del sistema judicial penal venezolano.

Se revisaron diversos artículos, material y estudios previos para sustentar la investigación con bases sólidas. Entre ellos, la Universidad Europea (UE, 2024), con un artículo intitulado “¿Qué es la evidencia digital? Características y tipos”, se destaca la definición de la definición de evidencia digital como cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático y fundamental para resolver muchos delitos y que resulta esencial en cualquier juicio penal.

De la misma forma, la Universidad Europea específica, en cuanto a las características de la evidencia digital, que la misma puede clasificarse en volátil (temporal) y no volátil (permanente). Tiene características únicas similares a las huellas dactilares y ADN, y puede ser alterada fácilmente. Además, puede duplicarse y verificar su integridad con herramientas



adecuadas e igualmente, señala que la evidencia digital pueden clasificarse según el tipo de elemento (hardware), sistema (abierto, telecomunicaciones, convergentes), y origen (generada por ordenador o persona).

Asimismo, indica la Universidad Europea que el proceso de manejo de evidencia digital sigue pasos como preservación, identificación, documentación, recopilación, obtención y análisis. Debe cumplir con autenticidad, integridad, fiabilidad y conformidad con normas judiciales para ser aceptada en procesos legales. Concluye, enfatizando que la evidencia digital es crucial en la resolución de casos legales, no solo delitos en la red. La tecnología plantea desafíos significativos para el derecho, especialmente en la obtención, preservación y análisis de estas evidencias, que requieren técnicas especializadas de informática forense.

De la misma forma, citando el artículo realizado por Mendoza (2024), titulado: “Interpretación y Desafíos de la Evidencia Digital en la Investigación Criminal”, en el mismo se destacan cómo los avances tecnológicos afectan la práctica forense debido a que herramientas modernas y las técnicas de análisis han avanzado significativamente enfrentándose desafíos importantes como la obsolescencia tecnológica, problemas de autenticidad y manipulación de la evidencia, así como dificultades en la extracción de datos debido a la encriptación y el uso creciente de la nube.

Por su parte, Álvarez (2024), en un artículo, intitulado “Tratamiento de la evidencia digital en Venezuela. Aspectos de consideración” señala que, la cadena de custodia es el proceso que asegura la integridad y autenticidad de las evidencias desde su obtención hasta su disposición final. Es fundamental para evitar la alteración o contaminación de las pruebas.

Además, Álvarez concluye que el Manual Único de Cadena de Custodia de Evidencias Físicas de Venezuela detalla los procesos para asegurar evidencias físicas, pero no aborda adecuadamente las digitales y que se requiere un esquema específico para el manejo de evidencias digitales,



siguiendo prácticas internacionales para asegurar su integridad y autenticidad.

La evidencia digital: Se refiere a cualquier dato originado, almacenado o transmitido por medios digitales, utilizado para demostrar hechos punibles en proceso judicial. Según Presman (2016), la evidencia digital, es cualquier tipo de dato almacenado en un dispositivo informático que los peritos deben recoger en la escena del crimen digital. Por su parte, Ortiz (2019), expresa, la evidencia digital son “todos aquellos datos aislados o relacionados entre sí que poseen características esenciales de recuperabilidad, preservación y demostración de sus existencia.” (p.1).

Posibles evidencias digitales: correos electrónicos, historiales de navegación, Chat, fotografías en distintos formatos archivos (JPG, PNG, GIF, BMP, TIF), archivos de imágenes, documentos, archivos de texto, metadatos de archivos, claves en memoria, claves de encriptación, entre otros.

Principios fundamentales de la evidencia digital: La evidencia digital debe cumplir tiene tres principios fundamentales la relevancia, la confiabilidad y la suficiencia, garantizando su admisibilidad en procesos judiciales.

Características de las pruebas o evidencia digital: Se consideran como características de las evidencias digitales las siguientes: a) Intangible, requiere de procesos informáticos para ser observada; B) Duplicable, puede ser copiada múltiples veces; c) Volátil, es susceptible de manipulación y alteración y E) Parcial, puede estar distribuida en múltiples archivos y ubicaciones.

Fases de la evidencia digital en el proceso judicial: la prueba digital pasa por tres fases dentro del proceso de cadena de custodia digital: 1) Obtención: Acceso a las fuentes de la prueba digital; 2) Incorporación: Inclusión de datos relevantes, garantizando su pertinencia, necesidad y licitud. 3) Valoración de los datos por el órgano juzgador.



Manejo de la evidencia digital como prueba en el proceso judicial penal.

En los procesos judiciales penales el manejo de la evidencia digital enfrenta diversos desafíos relacionados con su validez y eficacia procesal. A pesar del aumento en la jurisprudencia sobre su admisión como prueba, existen dificultades en garantizar su integridad, autenticidad y originalidad. La fecha de obtención y la cadena de custodia son cruciales para su admisión, pero la falta de métodos adecuados para verificar estos aspectos puede llevar a la desestimación o exclusión de la prueba digital incluso antes del juicio. Además, la capacidad de manipulación y creación digital plantea dudas sobre la autenticidad de las pruebas, lo que agrava la situación.

En Venezuela, en respuesta a estos desafíos, el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz, junto con el Gobierno Bolivariano, ha desarrollado un protocolo de cadena de custodia de evidencia digital, incorporado al Manual Único de Cadena de Custodia de Evidencias Físicas, firmado en diciembre de 2022. Este protocolo establece procedimientos estandarizados para el manejo de evidencias, incluida la digital, en consonancia con criterios científicos, forenses y jurídicos. Las evidencias digitales inicialmente no se registran en la Planilla Única de Cadena de Custodia de Evidencias, aunque sí tienen interés procesal. Ejemplos: Incluyen peritajes psiquiátricos, psicológicos, trazas telefónicas, perfiles financieros y registros documentales.

En conclusión, el manejo adecuado de la evidencia digital y la adherencia a los lineamientos y principios éticos establecidos son fundamentales para asegurar un proceso judicial justo y efectivo en Venezuela. En fin, la cadena de custodia garantiza la fiabilidad de la prueba digital que se aporta en un juicio. Sin embargo, su manipulación es fácil lo que hace ineludible la preservación adecuada de la autenticidad e integridad de las pruebas o evidencias digitales.



Objetivo General del Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela (2022), El compendio tiene como objetivo general, Estandarizar y orientar las actuaciones de los funcionarios y funcionarias, peritos (as), forenses, expertos (as), criminalistas de los órganos de policía de investigación; de los(as) fiscales del Ministerio Público; de los(as) defensores de la Defensa Pública; así como Jueces y Juezas del Tribunal Supremo de Justicia, investigadores (as) penales y especialistas del Ministerio Público, al igual que los (as) adscritos (as) a los órganos con competencia en materia de investigación penal en el desarrollo de los procedimientos criminalístico, técnicos, científicos y forenses, aclarar aspectos conceptuales, y explicar las consideraciones necesarias que deben realizar para avanzar en la garantía y el respeto de los derechos humanos en el proceso preparatorio de la investigación penal.

Alcance del Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela (2022). Además el compendio antes citado, tiene como alcance a todas las personas u operarios que participen en el tratamiento de evidencias físicas en cualquiera de las fases del sistema de cadena de custodia.

Definición de Operarios. Igualmente, en el compendio se instituye que entre los operarios(as), son personas facultadas para gestionar la Cadena de Custodia en la investigación penal. Entre estos operarios se incluyen: Jueces, Fiscales del Ministerio Público, Defensores Criminalistas, Forenses y Peritos, Investigadores Penales, Funcionarios Policiales y Militares en funciones de investigación penal, Bomberos y Rescatistas, Operadores del Sistema de transporte Metro, Médicos, personal de enfermería, de morgue y otros especialistas de centros de salud públicos o privados.

Bases legales del Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela (2022). Potencialmente, este compendio se fundamenta en diversas normas y convenios nacionales e internacionales, entre ellos los más notables:



a)Nacionales: Constitución de la República Bolivariana de Venezuela (Gaceta Oficial N° 36.860, 1999) y Enmienda N° 1 a la Constitución de Venezuela (Gaceta Oficial N° 5.908 Extraordinario, 2009) y B)Internacionales:1)Declaración Universal de los Derechos Humanos (1948); 2) Convención contra la Tortura y otros Tratos o Penas Cruelles, Inhumanos o Degradantes (1984, en vigor desde 1987); 3)Convención de Viena sobre Relaciones Diplomáticas (1961, en vigor desde 1964); 4)Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (1965, en vigor desde 1969); Pacto Internacional de Derechos Civiles y Políticos (1966, en vigor desde 1976); 5)Convención sobre la Eliminación de Todas las Formas de Discriminación Contra la Mujer (1979, en vigor desde 1981) y 6)Reglas Mínimas de las Naciones Unidas para la Administración de la Justicia de Menores (Reglas de Beijing, 1985).

Desde este marco referencial, con fundamento en el mismo Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela (2022), se establece que la tecnología de información es cualquier dato o información digital y el equipo tecnológico que lo contiene, susceptible de peritaje forense, pueda ser admitido como prueba en un proceso legal.

Las evidencias de Tecnologías de Información, Comunicaciones y Operativas se clasifican por su naturaleza en: 1) Evidencias en Dispositivo Digital (EvDD): Equipo electrónicos tangibles; y 2) Evidencias Digitales (EvSSD): Datos o información digital intangible almacenada o transmitida en binario, en un medio tecnológico de acceso directo, incluyendo texto, audio, vídeo, imagen y datos híbridos.

Tecnologías susceptibles de análisis forenses que pueda ser admitido como prueba en un proceso legal: 1).-Dispositivos computacionales portátiles o no, 2).-Sistemas de telefonía y comunicaciones móviles incluye accesorios, 3).Sistemas Satelitales de Navegación y de posicionamiento global: Como GPS, 4).- Drones, vehículos aéreos pilotados a distancia



(RPAS), 5).-Dispositivos de almacenamiento: Memorias flash, dispositivos ópticos, 6).-Dispositivos seguridad de redes: Enrutador, detector de intruso firewall, Switch y cualquier otro equipo que genere log, 7).-Sistemas de vigilancia y reconocimiento: CCTV y dispositivos de vigilancia para almacenar o transmitir video y Otras tecnologías relevantes: a)Internet de las Cosas (IoT): Sistemas interconectados con aplicaciones para activar o desactivar equipos. b) Blockchain: Tecnología de cadena de bloques, c)Realidad aumentada y virtual, d)Inteligencia artificial y aprendizaje automático, e) Computación en la nube: Todo tipo de almacenamiento y servicios en la nube, f) Computación cuántica, g)Robótica, h) Redes Sociales, Portales Web y Correo Electrónico

Tecnologías Operativas: Las infraestructuras críticas, también conocidas como estratégicas, son esenciales y no tienen alternativas. Su perturbación o destrucción tendría un grave impacto. Ejemplos incluyen servicios eléctricos, transporte masivo, gas, petróleo y defensa. La inclusión de tecnologías en esta categoría es flexible y se adapta a nuevas tendencias tecnológicas.

La cadena de custodia digital: es el procedimiento que permite de manera inequívoca conocer la identidad, integridad y autenticidad de los vestigios o indicios digitales relacionados con un hecho punible o acto delictivo, desde que son encontrados o se inicia la indagación hasta que se aportan al proceso judicial para ser valorados como pruebas, es decir la cadena de custodia, es el conjunto de actos que asegura la autenticidad e inalterabilidad de las pruebas, desde su recolección hasta su presentación en juicio.

Según Suarez (2008), la cadena de custodia, es el sistema, de control y registro que se aplica al indicio, evidencia, objeto, instrumento del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente ordene su conclusión. La cadena de custodia, incluye: La Extracción/ Recolección:



Obtención de los indicios; Preservación y Embalaje: Asegurar su Integridad y Custodia Final: Mantenimiento hasta el juicio.

La finalidad de la cadena de custodia: Es garantizar la exacta identidad de lo incautado y de lo analizado. Por tanto, la cadena de custodia digital tiene un valor fundamental, puesto que sirve para certificar que lo analizado y presentado ante un tribunal como prueba es lo mismo que los indicios digitales recogidos. La cadena de custodia digital garantiza la fiabilidad de la prueba digital que se aporta en el juicio y la adecuada defensa mediante la correspondiente pericial informática. Resulta imprescindible dentro del procedimiento de prueba pericial informática/tecnológica, para garantizar su autenticidad e integridad, debido a que puede ser fácilmente manipulada. En consecuencia, si se sigue el correcto proceso de cadena de custodia digital se consigue evitar la contaminación de los medios probatorios.

Fases de la Cadena de Custodia Digital: 1) Identificación: Reconocer la evidencia digital relevante; 2) Preservación: Asegurar la integridad de la evidencia digital; 3) Extracción: Recuperar los datos necesarios; 4.) Análisis: Evaluar y examinar la evidencia digital; 5) Interpretación: Entender y explicar los datos recolectados y 6) Presentación: Presentar la evidencia en un formato comprensible en el juicio.

Pasos de la Cadena de Custodia Digital: a) Observación, b) Búsqueda, c) Fijación, d) Colección, e) Embalaje y Rotulado, y f) Registro de Cadena de Custodia. En conclusión, la cadena de custodia es esencial para asegurar que la evidencia digital sea admitida y valorada correctamente en un proceso judicial, garantizando su autenticidad e integridad.

Lineamientos y Procedimientos de la cadena de custodia digital: Lineamientos de consignación Primaria (obtención) y de Laboratorio y Procedimientos para asegurar la adquisición y análisis de la evidencia digital: Recepción, Designación, Peritaje y Remisión, procesos para gestionar la evidencia desde su recepción hasta su análisis y posterior envío.



Lineamientos generales y específicos establecidos: Evidencias Tecnológicas, Protección del sitio del suceso; Asegurar la integridad de la evidencia digital, manteniendo los dispositivos encendidos y deshabilitando señales de comunicación que puedan alterar los datos y Protección aplicada a sitios con elementos de interés criminalístico; Medidas preventivas para evitar la alteración de la evidencia digital por terceros. Por otra parte, el compendio de protocolo de evidencias digitales anexo se delimita el procedimiento de **Fijación Imagenológica**, como las técnicas avanzadas para capturar imágenes de elementos no visibles a simple vista, utilizando rayos X, tomografías, ultrasonido, entre otros.

Importancia de la Cadena de Custodia Digital: Garantizar la autenticidad y preservación de la evidencia digital. La correcta aplicación de protocolos y técnicas forenses asegura la integridad de la prueba digital y su admisibilidad en el juicio.

Ética y Procedimientos en la Investigación Penal: a) Aplicación de principios éticos, los investigadores deben seguir normas éticas rigurosas para garantizar la integridad del proceso y la protección de los derechos de los sujetos implicados y b) Legislación y Normativas: El compendio busca establecer una base sólida para el manejo de la evidencia digital, asegurando el cumplimiento de los principios rectores y procedimientos adecuados en la investigación penal.

Por otra parte la ruptura de la cadena de custodia digital puede generar dudas, lo cual trae como consecuencia que se descarte o excluya la admisión de la prueba por ser declaradas contaminadas, invalidas y no fiables, lo cual favorece la impunidad con la absolución de delincuentes que dejan pruebas en los dispositivos electrónicos u otros cibercriminales o viceversas que una persona inocente resulte condenada por un delito del cual es inocente o no cometió, generándose de este modo una sentencia afirmada en la doctrina de los frutos del árbol envenenado y por ende una inseguridad jurídica.



Al respecto, Pereira (2014), analiza las consecuencias de la prueba ilícita en el debido proceso, utilizando la metáfora bíblica del "fruto del árbol envenenado" (Mateo 7:17-20), que establece que una prueba ilícita contamina las evidencias derivadas de ella. También, Pereira señala que esta doctrina, se originó en Norteamérica con el caso *Silversthorne Lumber Co. vs. United States* (1920) y desarrollada en el caso *Nardone vs. United States* (1939). (P.71), y que protege los derechos fundamentales al excluir cualquier prueba obtenida ilícitamente o derivada de tales pruebas.

Argumenta, Pereira que la Constitución de la República Bolivariana de Venezuela, en su Artículo 49, numeral 1, declara nulas las pruebas obtenidas mediante violación del debido proceso, y el Código Orgánico Procesal Penal refuerza este principio, invalidando pruebas obtenidas por medios ilícitos. Cualquier prueba obtenida de manera ilegal y sus derivados son inadmisibles y pueden ser excluidas de oficio en cualquier etapa del proceso, por ser de orden público. En resumen, Pereira sostiene que la doctrina del "fruto del árbol envenenado" y las leyes venezolanas protegen el debido proceso al declarar nulas y excluir todas las pruebas obtenidas directa o indirectamente de manera ilícita, garantizando así la integridad del sistema judicial.

Aunado a ello Jiménez (2019), señala que el saber criminalístico, ávido de encontrar la verdad real, brinda una inestimable colaboración al proceso penal con el propósito de que el hecho delictuoso cometido no quede impune, puesto que comprueba científicamente la existencia del hecho punible, aporta determinaciones científicas relacionadas con la forma en que el delito se ha perpetrado, con la cronología, con los medios utilizados, con la individualización de la o de las personas intervinientes, con la concordancia entre las pruebas e indicios y la realidad de los hechos.

En efecto, la Criminalística dentro de sus fines, tiene como fin inmediato o próximo, establecer la existencia de un hecho presuntamente delictivo, reconstruirlo e identificar al autor o a los autores y como fin mediato o



último, suministrar a las autoridades los datos científicos y técnicos que conduzcan al ejercicio de la acción penal

Principios Éticos y Normativos: La ética es esencial en la investigación para asegurar la validez y fiabilidad de los resultados. Los investigadores penales deben seguir normas éticas rigurosas para proteger los derechos de los sujetos y la integridad del proceso y la aplicación adecuada de técnicas forenses permite esclarecer el delito y asegurar una investigación justa. La ética en la investigación penal es crucial para validar los resultados y asegurar que los peritos actúen profesional y responsablemente, respetando los derechos humanos y la integridad de los sujetos de investigación.

Según Dussel (2015), los investigadores deben seguir normas éticas para garantizar una investigación responsable y sin perjuicios. La ética en la investigación penal implica subsumir principios éticos generales en el campo específico de la investigación penal, garantizando que los derechos de los sujetos sean respetados y se eviten daños. Los principios éticos son subsumidos, metidos dentro, se subsumen analógicamente los principios de la ética los principios de la investigación penal se concretan se especifica los campos practico un principio de general ético.

En el campo de la investigación penal, parecería que tanto la ética como la moral están sobre entendidas, en la praxis de la acción penal, se trata de analizar críticamente de cómo los principios de la ética son subsumidos por los principios del campo de la investigación penal.

En el ámbito de la ética aplicada a las investigaciones penales, se han propuesto varios enfoques, entre ellos el deontológico y el de las virtudes. El enfoque deontológico se centra en los deberes y obligaciones que los funcionarios públicos deben cumplir en el desempeño de sus funciones, mientras que el enfoque de las virtudes se Enfocada en la formación del carácter y la adquisición de virtudes para tomar decisiones éticas en situaciones complejas.



Ambos enfoques son importantes para que los funcionarios actúen con integridad, transparencia y responsabilidad, basándose en principios éticos sólidos y en el bienestar de la sociedad. La ética destaca la importancia de reconocer y respetar la alteridad del otro, tratándolo con dignidad y respeto. En el contexto penal, esto es esencial para evitar tratar a las personas como medios para fines propios y asegurar un trato humano y justo.

Todos los involucrados en el tratamiento de evidencias digitales deben actuar con ética de virtudes y deontología para evitar la impunidad. Esto está alineado con los principios del Código Orgánico Procesal Penal: 1.) Principio de Legalidad de la Prueba: Garantiza el respeto a los derechos fundamentales en la obtención e incorporación de pruebas, y 2.) Principio de Libertad Probatoria: Permite probar hechos por cualquier medio legal.

Un mal manejo de las evidencias digitales puede romper la cadena de custodia, haciendo que la prueba se considere ilícita y no sea admitida en juicio. Esto subraya la importancia de la ética y la correcta gestión de las evidencias digitales para el éxito de las investigaciones penales.

Marco Legal y Protocolo: El Código Orgánico Procesal Penal establece principios como la legalidad de la prueba y la libertad probatoria. Un mal manejo de las evidencias digitales puede llevar a su inadmisibilidad en juicio, destacando la importancia del estricto cumplimiento de la cadena de custodia. En corolario: El manejo adecuado de las evidencias digitales y la adherencia a principios éticos y normativos son esenciales para garantizar un proceso judicial justo y efectivo, evitando la impunidad y protegiendo los derechos de todos los involucrados

Enfoque Metodológico: La investigación se centra en el uso de las herramientas tecnológicas, dispositivos electrónicos y la informática forense como medios esenciales para identificar la escena del delito y a los responsables. La investigadora adopta una perspectiva pospositivista con un enfoque cualitativo, que es humanista y busca entender la realidad social de manera evolutiva y negociada.



Según Crespi (2013), en el paradigma postpositivista, la realidad es objetiva pero nunca completamente aprehensible, existiendo independiente del investigador. La metodología cualitativa, como señala Martínez (2007), estudia la “naturaleza profunda de las realidades y permite construir una relación dialéctica entre la investigadora y el objeto de estudio” (p.8).

A partir de la naturaleza de investigación se presenta el tipo y diseño de investigación, el cual según Arias (2012) “es una estrategia a adoptar para responder al problema planteado”. (p.110). Desde esta perspectiva, el método de la investigación es de tipo hermenéutica, con un diseño documental de nivel descriptivo, buscando interpretar textos y fenómenos sociales. Este enfoque se afirma en técnicas como Categorización, Triangulación y Teorización para analizar la información compilada a través de las técnicas de recolección: fichaje, resúmenes lógicos y esquemas analíticos, las cuales facilitan la organización y análisis de la información.

La recolección de la información transitan varias etapas: Búsqueda de fuentes, lectura de documentos, elaboración de esquemas, recolección y análisis de información y construcción teórica. En el análisis se emplearán técnicas lógicas como inducción, deducción, análisis y síntesis, centrándose en el manejo de la evidencia digital y los estándares establecidos en el Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela” (2022).

La triangulación será crucial para minimizar sesgos y asegurar la validez y fiabilidad de los hallazgos. Se utilizan cinco procesos para el análisis: Categorización, Estructuración, Triangulación, Contrastación y Teorización, las cuales permiten interpretar y construir teorías a partir de la información recolectada, tal como lo establece Corral (2017).



Conclusión

a) El manejo adecuado de la evidencia digital es crucial para esclarecer delitos con precisión y sin errores, garantizando la integridad y autenticidad de la información usada como prueba en Venezuela; b) Venezuela ha avanzado en la creación del Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela (2022), que establece procedimientos estándar y obligatorios para todos los participantes en el manejo de la evidencia digital; c) Es necesario estandarizar estos protocolos para las personas involucradas en el proceso judicial, incluyendo jueces, defensores, peritos, investigadores, entre otros.; d) El protocolo incluye pasos específicos para proteger, observar, buscar, fijar, recolectar, embalar, etiquetar, preservar y trasladar la evidencia digital, alineados con la legislación y normas vigentes y e) La cadena de custodia debe asegurar la autenticidad e integridad de la prueba digital para que sea admisible en el proceso judicial, evitando su exclusión y garantizando una justicia efectiva.

Recomendación

Se insta a todos los involucradas en la cadena de custodia a actuar con ética y aplicar efectivamente las normas y procedimientos del Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela (2022); b) El Estado venezolano debe sensibilizar, capacitar y actualizar a todos los participan en el manejo de evidencias digitales para asegurar la correcta aplicación de los Protocolos; c) Es vital seguir los lineamientos generales y específicos del compendio para el manejo de la evidencia digital en el sistema de justicia penal venezolano; d) Aplicar estrictamente el compendio para mantener la autenticidad, integridad y confiabilidad de la evidencia digital, evitando errores que puedan alterar su valor probatorio en el proceso judicial penal. Y e)



Asegurar la preservación de la legitimidad de los elementos probatorios digitales, considerando su relevancia, confiabilidad y suficiencia para evitar la exclusión en el proceso judicial.

Referencias

- Álvarez, N. (04 de Enero de 2024). Tratamiento de la evidencia digital en Venezuela. Aspectos de consideración. [Texto en línea] Disponible: <https://blog.Juridicos venezuela.com/tratamiento-de-la-evidencia-digital-en-venezuela-aspectos-de-consideracion/>
- Arias, F. (2012). *El Proyecto de Investigación, Introducción a la Metodología Científica*. 6ta edición. Editorial Episteme. C.A.
- Código Orgánico Procesal Penal (2012). Gaceta Oficial de la República Bolivariana de Venezuela, N° 6.078 (Extraordinari0), Junio 15, 2012. Caracas.
- Constitución República Bolivariana de Venezuela*. (1999). Gaceta Oficial de la República Bolivariana de Venezuela, N° 5.453 (Extraordinaria), Marzo 24, 2000.
- Corral, Y. (2017). *Validez y Fiabilidad en Investigaciones Cualitativas*. [Revista en línea: ARJÉ Revista de Postgrado FaCE-UC.,11 (20), 196-209
- Cortes, L., Di Lorio, A., y Lagos, E. (Compiladores) (2020). *Nuevas Tecnologías en la Investigación Criminal: Aporte de la Informática a la Criminalística*. Cali: Universidad Libre-Universidad de Fasta
- Crespi, Ma. De la S. (2013). *Paradigmas de investigación y planos del conocimiento*. Disponible: <https://www.youtube.com/watch?v=YgUkwmCy2oY>.
- Dussel, E. (2015). *14 Tesis de ética*. Buenos Aires: Editorial Docencia.
- Jiménez, L. (2019). *Cinco pasos más importantes para el procesamiento de un lugar de los hechos*. Bogotá: Grupo Educativo MEI
- Londoño, Maldonado y Calderón (2014), *Guía para construir el estado del arte*. Bogotá: ICONK
- Manual Único de Cadena de Custodia de Evidencias Físicas. (Agosto de 2018). Gaceta Oficial de la República Bolivariana de Venezuela. [Texto en línea] Disponible: <http://www.mppriip.gob.ve/wp-content/uploads/2018/05/ManualDeCustodia.pdf>. [Consulta: Marzo 29, 2023].
- Martínez, M. (2007). *Investigación Cualitativa Etnográfica*. México D.F. Trillas.
- Martínez, G. (2022). Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología*, 24 (23),1-38.



- Mendoza, M. (2024). Interpretación y Desafíos de la Evidencia Digital. Código Científico. *Revista de Investigación*, 5(E3), 480-498.
- Ministerio del Poder Popular para las Relaciones Interiores Justicia y Paz (MPPRIUP, 06 de diciembre 2022). *Compendio de Protocolos de Actuación para el Fortalecimiento de la Investigación Penal en Venezuela*. Caracas, Venezuela. Disponible: http://www.Defensapublica.gob.ve/wpcontent/uploads/2022/12/COMPENDIO_PROTOCOLOS.pdf.
- Ortiz, E. (2019). *Evidencia Digital: Fundamentos Aplicables para el Abordaje de la Examinación Forense*. Bogotá: RedCiber- ASIIF
- Pereira, L. (2014). *Pruebas ilícitas y nulidades en el proceso penal*. (Concordada con el COPP de 12 de junio de 2012). (5ta ed.). Caracas. Editores: Vadell.
- Presman, G. (10 de mayo de 2016). *Desafíos de la Informática Forense. Aspectos que promueven una postura de investigador*. VI Congreso Iberoamericano de Docentes e Investigadores en Derecho e Informática, del 5 al 7 de mayo en la Facultad de Ciencias Jurídicas y Sociales (FCJS) y en la FICH. Universidad de Buenos Aires.
- Sanchis, E. (2018). *Qué son las evidencias digitales y cómo se obtienen*. Peritos Informáticos.
- Suarez, L. (2008). *Cadena de Custodia Guía Nacional Conferencias Nacional Conjuntas de Procuración de Justicia y de Secretarios de Seguridad Pública*. México D.F. Universidad Nacional Autónoma de México.
- Universidad Europea. (UE, 23 febrero de 2024). *¿Qué es la evidencia digital? Características y tipos*. [Texto en línea] Disponible: <https://universidadeuropea.com/blog/evidencia-digital/>
- Universidad en Internet (UNIR, 2021). *Informática Forense: en qué consiste, ámbito de aplicación y perfiles profesionales*. *Ingeniería y Tecnología*. [Texto en línea] Disponible: <https://www.unir.net/ingenieria/revista/informatica-forense/>.