La evidencia digital como medio de prueba en el Proceso Penal

Digital evidence as a means of proof in the Criminal Process

Miguel Angel Osco Escobedo
ORCID: 0000-0003-1885-3549
Universidad César Vallejo – Escuela de Posgrado - Lima - Perú
Correo: moscoe@ucv.edu.pe

Yolanda Maribel Mercedes Chipana Fernández
ORCID: 0000-0002-8609-3409
Universidad César Vallejo – Escuela de Posgrado - Lima - Perú
Correo: ychipana@ucv.edu.pe

Gladys Beatriz García Quispe
ORCID: 0000-0002-3064-7919
Universidad César Vallejo – Escuela de Posgrado - Lima - Perú
Correo: Ggarciaqu@ucvvirtual.edu.pe

José Joaquín Díaz-Pérez
ORCID: 0000-0003-1663-8626
Universidad César Vallejo – Escuela de Posgrado - Lima - Perú
Correo: josejoaquindiazperez33@gmail.com

Calvo De Oliveira Diaz, Deny Giovanna
ORCID: 0000-0002-8907-676X
Universidad César Vallejo – Escuela de Posgrado - Lima - Perú
Correo: denycalvo@gmail.com

Resumen

La evidencia digital es información archivada en un dispositivo tecnológico que se propala por medio del ciberespacio. El registro informático, es accesible por personas, la electrónica o informática y se recolecta de un dispositivo digital. Esta investigación tiene por objeto precisar el correcto tratamiento de la evidencia digital para ser admisible dentro del proceso judicial, respetando garantías y derechos fundamentales de las personas. Además identificar el procedimiento de obtención, preservación, análisis y presentación de la evidencia digital ante el Juez. Esta revisión teórica de fuentes se elaboró bajo la metodología de verificación sistemática, utilizable en base de datos Scopus, Ebscohost, Scielo, Core, Jurn, y Redalyc de configuración ventajosa y en español los últimos 5 años. Se empleó la exploración y revisión de producción científica, seleccionando las expresiones de: “proceso penal”, “evidencia digital” y “medio de prueba”. Sobre los resultados obtenidos se colige la importancia del tratamiento de la evidencia digital como instrumento de prueba, para la valoración del juez como elemento de convicción en un proceso penal. Se concluye que la evidencia digital posee características particulares que la distinguen de la evidencia física y las normas procesales no regulan su adecuado tratamiento, siendo considerada actualmente como prueba documental.

Palabras clave: Evidencia digital; medio de prueba y proceso penal.

_____

Abstract

Digital evidence is information stored on a technological device that is propagated through cyberspace. The computer record is accessible by people, electronics or computers and is collected from a digital device. The purpose of this investigation is to specify the correct treatment of digital evidence to be admissible within the judicial process, respecting guarantees and fundamental rights of people. Also identify the procedure for obtaining, preserving, analyzing and presenting digital evidence before the Judge. This theoretical review of sources was prepared under the systematic verification methodology, usable in the Scopus, Ebscohost, Scielo, Core, Jurn, and Redalyc databases of advantageous configuration and in Spanish for the last 5 years. The exploration and review of scientific production was used, selecting the expressions of: "criminal process", "digital evidence" and "evidence". Based on the results obtained, the importance of the treatment of digital evidence as an instrument of proof is inferred, for the evaluation of the judge as an element of conviction in a criminal process. It is concluded that digital evidence has particular characteristics that distinguish it from physical evidence and procedural rules do not regulate its proper treatment, being currently considered as documentary evidence.

Keywords: digital evidence; evidence and criminal proceedings

Introducción

Los diferentes grupos humanos han cambiado su forma de relacionarse influenciados por el apogeo de las tecnologías de la información y la comunicación. Al viajar por internet en el inacabable mundo de la información lo hacemos sin ningún tipo de obstáculos, sin fronteras entre países y continentes. Esto ha derivado que las personas dejen el anonimato comunicacional, para generar una fuente de comunicación que registra su paso por la red cuando realizan búsquedas, dejando rastros digitales que se alojan en registros informáticos que se convierten en evidencia digital, las cuales pueden ser empleadas en un proceso judicial. Las formas como hoy los ciberdelincuentes ejecutan sus actividades delictivas ha cambiado y evolucionado, resulta alarmante el empleo de las TIC en nuevos tipos de delitos que afectan a muchas personas y organizaciones en el mundo global. La evidencia digital ha generado una problemática jurídica al proceso penal, respecto a la adecuación de los mecanismos probatorios habituales con las recientes tecnologías, sumado a ello también se enfrenta a nuevos medios de prueba.

La evidencia digital en la actualidad es desconocida en el medio judicial, sobre todo por jueces, fiscales y los profesionales de Derecho (Rivero, 2018). La Organización Internacional de Evidencia Computacional asevera que la evidencia digital es información producida, transmitida o almacenada por soportes electrónicos que se emplea en procesos judiciales, en investigaciones internas de ciberseguridad, análisis de malware, etc. Las precisiones varían en función al objetivo específico de lo que se requiera procesar, podríamos citar como ejemplo, los procedimientos para obtener la transacción de un correo electrónico es distinto a las de obtener archivos de procesos de auditoria o logs en una base de datos (Ochoa, 2018). La evidencia digital tiene ciertas características que la hacen muy particular, son fáciles de duplicar y transmitir, endeble a ser modificada y borrada, contaminada por otros nuevos datos y sensible al tiempo, asimismo es transnacional y jurisdiccional, ya que rompe las fronteras físicas (Prayudi, 2020). Se suma el avance tecnológico generado por nuevas formas de almacenar información como en la nube,

surgiendo la nueva posibilidad de acceder a ella y obtener evidencia digital (Palomo, 2021).

Se requiere cambiar los paradigmas que encierran los medios de prueba y entender que la evidencia digital advierte de nuevos procesos distintos a las evidencias físicas; la evidencia digital requiere de procedimientos legales y técnicos que aseguren que su adquisición se encuentre documentada, resguardada y disponible para su uso y revisión (Del Valle, 2018). De lo expuesto, es importante precisar que la evidencia digital necesita de expertos con conocimiento de técnicas especiales. Debiéndose tomar en consideración las características de volatilidad, el cuidado de la recolección de archivos que en muchas ocasiones no son posibles de observar, así como saber qué información se va a almacenar, ya que presenta formatos a veces complicados de entender, por lo que requiere traducción tecnológica para ser calificada por los operadores del sistema penal o las partes (Rodrigo, 2021).

Al respecto, el procedimiento de la admisibilidad de la evidencia digital es el eje central de la investigación. Existe cantidad de procesos que originan lagunas como consecuencia de la aplicación de la normativa procesal escrita para la evidencia física, y no para la evidencia digital (Piccirilli, 2019). A ello se suma el analfabetismo digital y la brecha tecnológica de los profesionales en el derecho. La administración de justicia requiere de profesionales informáticos preparados que examinen y cotejen las pruebas aportadas por las partes, dentro del entorno informático, protegiéndolas de las modificaciones a las que se exponen, dándole un entorno de autenticidad en la fase probatoria, y auxilio a los operadores de justicia, incorporando conocimiento técnico en el uso de los medios digitales (Alfonso, 2021). En el Perú no existe norma procesal que estandarice la recolección, obtención, conservación y análisis de la evidencia digital, asimismo la carencia de tecnología de dispositivos informáticos, aplicaciones, licenciamiento; y la demora en el trabajo de pericias sobre evidencia digital; así como la falta de formación de los operadores de justicia y cuerpos policiales, en técnicas de tratamiento de la evidencia digital, respecto a la obtención, recolección, conservación y análisis, que permitan asegurar su originalidad (Silva, 2021).

Asimismo, la importancia de la investigación es conocer el adecuado tratamiento de la evidencia digital en todas sus fases y la apropiada aplicación de la normatividad procesal por parte de los operadores de justicia. Finalmente, la investigación busca establecer los procedimientos normativos del correcto tratamiento de la evidencia digital, así como determinar la diferencia entre la evidencia física y la evidencia digital en la norma procesal y los procedimientos para la obtención, preservación, análisis y presentación de la evidencia digital.

Metodología

El presente estudio se efectuó bajo el enfoque cualitativo, mediante la revisión sistemática de producción científica relacionada con el tema de investigación, abordándose la búsqueda de información en revistas indexadas de Scopus, Ebscohost, Scielo, Core, Base, Jurn, Redalyc y tesis académicas, habiéndose tenido como principio la búsqueda por las palabras clave; *Evidencia Digital, Medio de Prueba y Proceso Penal.*

Se realizó un rastreo conceptual empleando menciones de estudios preferentes y complementarios hallados en los resultados de búsqueda digital. Las indagaciones se efectuaron en base de datos Scopus, Ebscohost, Scielo, Core, Base, Jurn, Redalyc y tesis académicas,

habiéndose tenido como principio la búsqueda por títulos, síntesis y por las palabras clave; Evidencia Digital, Medio de Prueba y Proceso Penal. Se desarrolló en el ámbito de una verificación estructurada de artículos de elaboración científica, el cual contenía: identidad del autor o autores, año, denominación, origen, DOI y menciones. El alcance de datos se realizó en una temporalidad no mayor de 5 años.

El proceso de recopilación de las investigaciones científicas fue efectuado por el investigador. Los estudios se escogieron referenciado dos periodos. Siendo el primer avance el reexaminado de títulos y síntesis de citas halladas con variados operadores de búsqueda de información y contraste mediante operadores lógicos boléanos, AND y OR vinculándose la evidencia digital como medio de prueba en el proceso penal. De la búsqueda sistemática y combinación se obtuvo una muestra de 52 resultados. El segundo avance se efectuó explorando el texto completo de las investigaciones seleccionadas para ratificar su elegibilidad, dando un total de 27 artículos.

Fueron excluidas aquellas verificaciones de literatura de creación teórica que no formaron parte del tema de investigación. Se apreció una restringida cantidad de investigaciones sobre evidencia digital como medio de prueba en el proceso penal, el objetivo de esta reseña es analizar los conocimientos existentes sobre el tema en mención e identificar en los productos de estudio, los diseños de formación, clases, variables y ponderaciones. Se escogieron como productos principales: indagaciones empíricas, sucesos de estudios, experiencias y semejantes.

Resultados

En la siguiente tabla se describe cada uno de los artículos seleccionados atendiendo su relevancia:

Autores/ Año/ Titulo	Tipo de Estudio	Métodos	Resultados	Conclusiones
Piccirilli, M. (2019). Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos: legislación vigente, anteproyectos y Convenio de Budapest.	Estudio cualitativo	Descriptivo - Comparativo	Las huellas digitales quedan guardadas en registros y podrían emplearse como evidencia digital en el proceso judicial.	La evidencia física no es igual a la evidencia digital. Por ello debe modificarse la legislación procesal respecto a la obtención de evidencia digital.
M. Rodrigo, F. (2021). La evidencia digital en el proceso penal y la preservación de los derechos fundamentales.	Aplico un estudio cualitativo	Métodoanalítico jurídico	La evidencia digital son datos almacenados en formato digital por medios tecnológicos, que podrían tener valor probatorio.	Necesidad de una norma que reglamente los procedimientos por el cual el Estado no invada el ámbito de privacidad, al localizar medios probatorios para llegar a resolver un hecho criminal.
Herrera, J. (2021). Estudio de la prueba electrónica, su preservación, adulteración, mecanismos de defensa y valoración en el proceso judicial.	Estudio cuantitativo descriptivo	Deductivo	La concepción de prueba electrónica como documento, equivalente a la prueba física en Colombia.	Herramientas, como IP, hash, laimagen forense, servidor, nube que podrían ser empleados en los litigios penales.
Parra-Sichaca, D. (2019). Requisitos jurídicos para la validez jurídica de la prueba digital.	Estudio cualitativo	Descriptivo - Comparativo	Las evidencias son pruebas digitales, que se utilizan en un proceso judicial. Para ser admitidos deben cuidarse respecto a su manejo.	Mantener un conocimiento de las normas y su reglamentación legal afiliada de las pruebas y el derecho procesal y las técnicas que genere seguridad jurídica en la información digital obtenida.
Del Valle, D. (2018). Evidencia Digital.	Estudio cualitativo descriptivo	Descriptivo	Existen códigos procesales que admiten el uso de medios de prueba electrónicos.	Es necesario, acercarse al problema de utilidad de la obtención, conservación, presentación y validez de las pruebas en el proceso judicial.

Schirakian, N. (2021). Evidencia informática: ¿un nuevo paradigma para el derecho procesal penal?	Estudio básico y de enfoque cualitativo	Métodoanalítico jurídico	Los Códigos Procesales no han previsto la incorporación de la evidencia digital en las investigaciones penales. Se incorpora este tipo de evidencia por el principio de libertad probatoria, mediante la analogía como herramienta principal.	La falta de regulación genera conflicto entre los derechos de los individuos expuestos al proceso penal y los mecanismos no regulados por el Estado.
Quevedo y Zamora (2022). El protocolo de reconocimiento de medios digitales frente a la inobservancia del debido proceso penal.	Estudio básico de enfoque cualitativo.	ExegéticoJurídico	La información digital adhiere hechos en la investigación fiscal, que se introduce en el proceso como prueba, no cumpliéndose reglas procesales.	La formación de profesionales del Derecho, debe realizarse en respeto a los derechos fundamentales de las personas y al debido proceso sobre la prueba, en la observación de grabaciones digitales, como medio de prueba.
Afonso, S. (2021). La prueba electrónica en el proceso penal.	Aplico un estudio cualitativo.	Descriptivo	El análisis de la prueba electrónica durante el proceso penal, pueden ser empleada por las partes, así como las gestiones de investigación de su obtención en el desarrollo de la investigación judicial o policial.	La prueba electrónica puede ser objeto de manipulación, al igual que la prueba convencional, ya que los medios tecnológicos son diversos actualmente de tal forma que ninguna prueba pueda escapar de esta posibilidad.
Muhammet, A., Morina, M., y Papajorgji, E. (2021). Digital Evidence and Prohibitions of Evidence Evaluation.	Estudio cualitativo	Descriptivo	La evidencia digital es un medio de prueba que puede emplearse para conocer la verdad material de un hecho pasado.	La evidencia digital es apta para la manipulación, intangible, invisible y virtual. Por ello, la obtención de pruebas de dispositivos digitales exige experiencia y debe realizarse desde un procedimiento.
Prayudi, Y., Ashari, A., y Priyambodo, T. (2020). The Framework to Support the Digital Evidence Handling: A Case Study of Procedures for the Management of Evidence in Indonesia.	Estudio cualitativo	Descriptivo	En una investigación el manejo de la evidencia digital, recibe igual tratamiento que la evidencia física.	La evidencia física y digital son evidencias en un proceso de investigación sobre casos de ciberdelitos.
Silva, G. (2021). La obtención de la prueba digital en los delitos informáticos en el distrito fiscal de Lima Norte.	Estudio Cualitativo	Análisis Teórico	El procedimiento de obtención de la evidencia digital se efectúa mediante la identificación, recolección, obtención conservación y análisis de la prueba digital, siendo necesario implementar un Protocolo práctico y aplicable.	Se requiere una Guía para la obtención, recolección, conservación y actuación de la prueba Digital, para uniformizar criterios y conocimiento en la investigación.
Cenci, M. (2021). Los desafíos penales de la evidencia digital.	Estudio cualitativo	Descriptivo	En materia penal la evidencia digital debe analizarse desde el derecho constitucional, penal y procesal penal, como herramienta de litigación y medio de prueba, entre otras.	La evidencia digital, no cuenta con protocolos y legislación, escaza jurisprudencia y doctrina.
Ochoa, P. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación.	Aplico unestudio cualitativo.	Descriptivo - Comparativo	El tratamiento de la evidencia digital es necesario en la investigación forense, mediante el análisis y las mejores prácticas.	La evidencia digital permite conocer la organología de ataques internos y/o externos, a fin establecer las medidas correctivas y seguir los procesos judiciales.
Espinoza, V. (2021). Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima.	Aplico unestudio cualitativo.	Descriptivo -	La ciberdelincuencia viene generando nuevas formas de delinquir, los códigos penales de varios países tienen vacíos, ello requiere de la aplicación de normas más contundentes y de la preparación del personal que investiga.	El sistema judicial no otorga el valor probatorio a la evidencia digital en los delitos informáticos, debido a la falta de valoración de la evidencia digital que en muchos casos se desestima, por la falta de cuidado en su tratamiento.
Molina, C., Beltrán, L., y Contreras, O. (2021). La Prueba Electrónica y Digital Aclaración de las diferencias jurídicas en Colombia.	Estudio cualitativo descriptivo	Comparativo jurídico Exegético	Las pruebas pueden ser testimoniales, documentales o digitales, que pueden utilizarse en un proceso judicial, para su admisión se deberá tener cuidado con su manejo, ya que pueden contaminarse y perder su valor probatorio.	Una prueba informática tiene como componente técnico un ordenador, donde se guarda información, como imágenes, videos, audios y blogs. La prueba digital es toda información almacenada y trasmitida de manera digital.

Estupiñan, T., Mora, K., y Santiago, C. (2019). Importancia de la Memoria como Evidencia Digital en la Informática Forense.	Estudio cualitativo	Deductivo	La relación entre la memoria y el manejo de la evidencia digital en una investigación forense, se fundamenta en el análisis de técnicas, metodologías y herramientas que faciliten la recopilación de información forense.	La evidencia digital es volátil, debe controlarse frente a un incidente a través del monitoreo y análisis de la red, con herramientas necesarias y políticas, para lograr generar una evidencia digital que sea admisible ante la corte.
Gómez, D., Acevedo, J., y Aguirre, J. (2021). Autenticidad y debido proceso en los mensajes de WhatsApp: Una revisión en los casos de divorcio	Estudio cualitativo	Descriptivo	La evidencia digital es fácil de modificar, por lo que es necesario verificar la autenticidad. El código hash es una herramienta que ayuda a garantizar la autenticidad de la prueba digital.	Los jueces dan pleno valor probatorio a pruebas aportadas de manera impresa en papel, sin verificar la autenticidad de la evidencia.
Samonova, V. (2022). Electronic Evidence in Administrative Proceedings. Cuestiones Políticas.	Estudio cualitativo descriptivo	Comparativo	Documentos en soportes de papel, requieren especial atención en su revisión y análisis para determinar su autenticidad.	Los tribunales administrativos debe emplear la prueba electrónica, ya que será el principal tipo de prueba en un futuro próximo.

Tabla 1: **Autores de textos y de revistas científicas indexadas cuyos contenidosfortalecen el tema de estudio**
Fuente: Elaboración propia

La primera investigación contenida en la tabla 1, concierne al artículo desarrollado por Piccirilli; realizado en Argentina. Estudio cualitativo y aplica el método descriptivo y comparativo. Indica que puede inferirse en todo lo que faculte ayudar para el hallazgo de la verdad, en relación con los hechos materia de investigación, que se procura actuar con la ley sustantiva. Concluye, que la evidencia física no puede igualarse a la evidencia digital, y que no puede aplicarse semejantes normas procesales.

El segundo estudio desarrollado en Brasil, de autoría de Rodrigo. Investigación cualitativa, y método analítico jurídico. Refiere que son diferentes formas de quienes participan en el proceso penal que pueden acceder y guiar al procedimiento los entendimientos requeridos, verdaderos o posibles, sobre la hipótesis a indagar y conocer, más las medidas restrictivas que las normas facultan para llevarlas a cabo. Concluye que los ámbitos digitales encierran espacios de privacidad de las personas y que la intromisión estatal deberá estar fundada y ordenada por autoridad judicial en el proceso penal y con elementos objetivos que lo sustenten.

El tercer artículo de Herrera se realizó en Colombia. Es un análisis que abarca una gran cantidad de pruebas dentro de las que se halla la evidencia digital. Concluye que, los intervinientes en un proceso judicial deben enterarse de las diferentes herramientas tecnológicas que pueden utilizarse en los litigios.

La cuarta publicación desarrollada por Parra en Colombia. Estudio de tipo cualitativo descriptivo. Menciona la diferencia marcada entre la fuente de prueba y medio de prueba, el primero, corresponde a herramientas que el Juez emplea para verificar las aseveraciones fácticas de las partes y son los previstos, con carácter restringido por el legislador, el segundo, concierne a los documentos, las partes, el testigo, lo que va a hacer examinado, y el saber técnico del perito. Concluye con la necesidad de conocimiento de normas legales afiliadas a las pruebas y el derecho procesal, y de técnicas que posibilite la seguridad jurídica en la información digital recogida.

La quinta publicación científica del autor Del Valle, estudio desarrollado en Argentina. El planteamiento metodológico cualitativo y descriptivo. Define que los criterios de fuente de prueba y medios de prueba, conciernen a la rama de análisis del Derecho procesal. La fuente delimita aquello que coexiste en la realidad, indistintamente de la existencia de un proceso; el medio es una noción que explica como dichas fuentes de prueba se consiguen incluir de manera segura dentro del proceso. Concluye que la obtención e incorporación de evidencia digital como prueba en juicio, demanda validación de peritos informáticos, que garantice que se obtuvo sin infringir el

derecho a la privacidad e intimidad de las personas.

El sexto estudio de Schirakian, investigación efectuada en Argentina. Análisis cualitativo de método descriptivo. Observa que en los Códigos Procesales Penales, no se señala los medios de prueba para poder admitir la evidencia digital a las investigaciones penales. Ante la falta de regulación, las autoridades judiciales adhieren este tipo de evidencia mediante el principio de libertad probatoria, empleando la analogía como instrumento principal. Concluye que las nuevas medidas probatorias, no se hallan reguladas, se emplean bajo el principio de libertad probatoria.

El séptimo apartado de Quevedo y Zamora en Ecuador. Metodología cualitativa, analítico jurídico. Enfatiza sobre el debido proceso que es obligación de los Estados, aplicar en materia penal mediante la actuación de garantías procesales que debe cumplir el Ministerio Público, demandada por la defensa técnica del sujeto pasivo y activo, debiendo ser analizadas y valoradas por los jueces que dictan sentencias. Concluye que videos, datos, fotografías son instrumentos de uso por el ciudadano, incluyendo el registro en un celular que graba hechos constituye fuente de prueba.

El octavo artículo de Afonso, se elaboró en España. Precisa que las pruebas generadas por medio de las TICs, al realizarse la recolección de la evidencia, se vulnera el derecho a su intimidad de la persona, accediéndose a datos personales sensibles que archivan sobre su ambiente íntimo y que no guarda relación con el hecho; así como la inviolabilidad del domicilio, al encontrarse el dispositivo dentro del ambiente calificado como domicilio y también el derecho al secreto de las comunicaciones, interceptándose mensajes entre dos o varias personas. Concluye que la prueba electrónica puede ser objeto de manipulación como cualquier otra prueba convencional, pero sin embargo, la prueba generada tecnológicamente muestra información precisa y completa.

La novena investigación, desarrollado por Eren y Mensur; elaborado en Turquía. Las evidencias digitales son de esencia abstracta en relación con otras pruebas clásicas y solo se hallan en sistemas digitales. Cuando la evidencia física se elimina o cambia, resulta más elemental de entender que la evidencia digital. Muy por el contrario, la manipulación de la evidencia digital puede ser más complejo de conocer. Por lo que a diferencia de la evidencia convencional, recolectar, preservar, analizar y evaluar evidencia digital es más complicado y oneroso. Concluyen, que la característica más significativa que diferencia a la evidencia digital es que es manipulable, intangible, invisible y virtual.

El décimo artículo investigación desarrollada en Indonesia, por Praduyi, Ashari y Priyambodo. Exploración cualitativa y aplica el método descriptivo. La evidencia digital y la evidencia electrónica con frecuencia se confunden y se utilizan, tanto en la praxis como en la teoría, con la ascendente complejidad y problemática del cibercrimen, que se debe comenzar a diferenciar. La evidencia electrónica es física, identificable por la vista y puede describirse. La evidencia digital es prueba en forma de archivos binarios. Ambos tipos de evidencia son el resultado de la obtención de discos y el proceso de generación de imágenes de evidencia electrónica o archivos con información digital significativa para la actividad de investigación. Concluyen que la evidencia física y digital es una unidad de evidencia en el proceso de investigación de casos de delitos cibernéticos.

El décimo primer estudio elaborado por Silva en Perú. Enfoque de tipo cualitativo y análisis teórico. La evidencia digital se define como toda información conseguida mediante un dispositivo digital en variados formatos de videos, imágenes, audios, redes sociales, información de correos electrónicos, y otros, la cual será fundamental en las investigaciones de Delitos Informáticos. Concluye que los problemas de acción probatoria de la prueba digital, se refieren a cuestionamientos sobre el recojo de la evidencia digital, la cadena de custodia, y la acertada manipulación del dispositivo que guarda la evidencia digital.

La décima segunda investigación de Cenci, fue redactado en Argentina. Enfoque metodológico empleado es cualitativo y descriptivo. La evidencia digital no solo se puede obtener como consecuencia de un allanamiento y de la pericia de un medio informático. Cabe la posibilidad de recabar este medio de prueba al efectuar la investigación, recogiendo datos como tags, logs y metadatos que los usuarios de la red dejan cada vez que se conectan a la red. Concluye que la falta de protocolos, la ineficiente legislación sobre el tema, la falta de jurisprudencia y doctrina especializada sobre la evidencia digital, son falencias que se tienen que enfrentar y solucionar.

La décima tercera investigación de Ochoa, estudio elaborado en Ecuador. Análisis cualitativo de método descriptivo comparativo. La evidencia digital podemos calificarla como volátil referente a una información temporal. No volátil refiere a información permanente en la memoria, tal como pendrive, disco duro, etc.; esta información permanece almacenada aun cuando se apaga el dispositivo. Concluye que se requiere un proceso estructurado del tratamiento de evidencia, que faculte aprender de los sucesos de seguridad y judicializarlos; con una cooperación internacional que permitan la protección de los registros.

El décimo cuarto artículo estudio desarrollado en Perú, por Espinoza. Indagación cualitativa y método descriptivo. El elemento de prueba puede denotar una causa concluyente en un proceso judicial, pero la singularidad de la evidencia digital está representado por el nivel de manipulación a la cual están exhibidas, puesto que están preparadas a partir de medios informáticos, que son empleados por las personas. Concluye que se logró determinar una relación entre los delitos informáticos y los procedimientos efectuados que aseguran el valor probatorio de la evidencia digital.

El décimo quinto estudio de los autores Molina, Beltran y Contreras en Colombia. Nos menciona un acápite de relevancia el cual denomina la triple carga en relación con la evidencia digital, siendo el primer aspecto que la evidencia digital debería saber recogerse, trasladarse y custodiarse adecuadamente para confirmar que es prueba legítima, que no está alterada y que sea segura respecto a su validez y eficacia procesal. El segundo aspecto refiere a la parte procesal de la evidencia digital, de saber incorporarlo correctamente en el proceso. Un tercer aspecto es cómo se reacciona cuando impugnan la evidencia digital que pudiere perjudicar el interés de nuestro patrocinado, ante ello como abogados debemos conocer cómo debatir y demostrar que la prueba es oportuna y necesaria en la valoración que tenga a bien el juez determinar en el proceso. Concluye que la prueba electrónica, comprende de una parte tecnológica, otra digital e informática, cubriendo el elemento lógico y el elemento material de la prueba, en referencia al software y hardware.

El décimo sexto artículo de Estupiñan, Mora y Santiago en Colombia. Alcance cualitativo deductivo. Hace referencia que la informática forense tiene como competencia fundamental recolectar evidencia suficiente para ser empleada en un proceso y servir de razonamiento en contra de los cibercriminales, a fin de conocer el legítimo causante del hecho, a través del empleo de herramientas y técnicas para analizar, identificar, reconstruir y recuperar la información acopiada durante la investigación. Concluye que la información que pasa en la red es volátil, para esto se debe contar con herramientas necesarias que logren generar una evidencia digital admisible ante la corte.

El décimo séptimo trabajo de Gómez, Acevedo y Aguirre, estudio desarrollado en Chile. Sseñala que para comprobar la integridad, así como la autenticidad de la evidencia digital, deberá emplearse la herramienta denominada código hash, algoritmo que permite confirmar que la información hallada en el medio digital original al momento de su ocupación no ha sido manipulada. El código hash es ideal para asegurar las evidencias digitales. Concluye que el código *hash* es un algoritmo matemático que asegura que las pruebas digitales no se encuentran alteradas ni

modificadas.

El décimo octavo artículo de Samonova en Ucrania. Metodología cualitativa, comparativo. Los tribunales consideran el valor probatorio de los metadatos y las posibilidades en contra de no utilizarlos. Los metadatos denominados datos de los datos son muy útiles para demostrar su admisibilidad y confiabilidad. Concluye que la prueba electrónica se utiliza de forma incierta y caótica, sin considerar sus prestaciones y características.

Discusión

Del análisis del inicio de los resultados, nos queda muy claro del buen sentido y uso que la tecnología nos brinda, mediante dispositivos digitales con mejores performances y bondades, con una infinidad de plataformas y aplicaciones empleadas para diferentes actividades que realiza el ser humano. La otra cara de la moneda es el empleo de las tecnologías por parte de personas que viven al margen de la ley, mediante la comisión de delitos a través de estos medios, que su accionar siempre genera rastros en la red denominados evidencia digital, que es nuestro tema de estudio. Considero la importancia de proteger la privacidad y la intimidad de las personas y hacerles frente a los cibercriminales mediante un proceso judicial que garantice su juzgamiento y sanción penal y para ello resulta vital contar con el medio de prueba que lo incrimine. Este elemento se ubica en el dispositivo tecnológico de la víctima o de su agresor, el cual se debe obtener, conservar y presentar en el proceso judicial. Sobre el particular, esta problemática exige contar con normas penales y procesales adecuadas respecto al tratamiento de la evidencia digital, así como un sistema judicial y policías preparados acorde a las modernas exigencias en materia digital, con igualdad de oportunidades para las partes dentro de un proceso judicial.

Pero antes de referirnos a la evidencia digital en nuestro estudio debemos precisar claramente que entendemos por la prueba en el contexto del proceso penal. Para tal efecto debemos señalar que la prueba requiere la necesidad de ser examinada y comprobada con todo objeto que la relaciona al hecho, con el fin de conocer lo más cerca posible la verdad de las circunstancias que se investigan. Apreciemos el concepto desde el ángulo del proceso, donde las partes acceden y se conducen conociendo los procedimientos como los testimonios, pericias y otros sobre los hechos, materia de investigación dentro del proceso penal, siendo de gran utilidad para el juez al permitirle un mejor conocimiento del proceso. Es pertinente precisar que el medio de prueba será admitido si cumple con los preceptos de respeto de los derechos y deberes fundamentales de las personas.

Es importante establecer la diferencia entre fuente de prueba y medio de prueba; en lo que concierne a la fuente de prueba estos son componentes que existen en la realidad desprendiéndose el objeto de prueba y nace lo que se debe probar, por ejemplo testigos, documentos, peritos, etc. En lo que se refiere al medio de prueba, es claro afirmar que es todo procedimiento que busca incorporar dentro del debido proceso los objetos de prueba en relación con los hechos que orientaran al juez una mejor convicción en el juzgamiento, por ejemplo, la confesión de las partes, la prueba documental, informes periciales, etc. Resulta relevante señalar y enfatizar sobre el debido proceso, al explicar que como derecho fundamental de las personas se exige al Estado la obligación de aplicarla de manera justa e imparcial por parte del juez. El Estado debe proveer las garantías mínimas para asegurar un juicio justo y acceso permanente y libre a la información y documentos resguardados por el sistema judicial.

Con relación a los medios de prueba en la admisión de la evidencia digital, debemos precisar que ante la falta de regulación en la legislación procesal se genera la necesidad de incorporar el principio de libertad probatoria, siendo la analogía su fundamento. Al respecto, comparto esta posición, ya que por la necesidad y ante la ausencia en los Códigos Procesales Penales del tratamiento de la evidencia digital, estas fueron creadas para admitir evidencias físicas. Este principio de libertad probatoria establece la facultad de emplear cualquier medio de prueba, con la viabilidad de la ley, siempre que no transgreda las garantías y derechos de la persona, las

facultades de los sujetos procesales, para poder incorporarlo como medio de prueba análogo.

La búsqueda de información en el Internet es frecuente y necesaria, desde la publicación de fotografías, historias en las redes sociales, búsquedas académicas de información por estudiantes de los diferentes niveles, comercio en línea, etc. y podríamos seguir enumerando las infinidades de empleo que tiene la búsqueda de información en la red. Analicemos como la justicia y los policías también se sirven para sus investigaciones de la búsqueda de información, sobre todo si esta es realizada en fuentes abiertas sin vulnerar los derechos fundamentales de las personas mediante el OSINT y el SOCMINT. Estas nuevas formas de hallar información a través de estas herramientas permiten acceder a información de personas que son parte del proceso y obtener evidencias digitales, como nombres de personas, teléfonos, direcciones, empleos, viajes, comentarios, etc. Es por ello que esta información o rastro digital que dejan los usuarios por su navegación en el Internet puede ser empleada en la investigación penal inicial, bien para corroborar hechos o excluirlos del mismo. Es por ello que las evidencias digitales son distintas a las evidencias clásicas, ya que solo pueden ser halladas en relación directa con el empleo de dispositivos digitales y aplicaciones o plataformas alojadas en la red como información, configurando de esta forma una particularidad a diferencia de las evidencias clásicas. Por citar un ejemplo al eliminar o borrar datos estos pueden ser recuperados mediantes técnicas forenses en comparación a la evidencia clásica que no es posible.

Por otro lado, es importante precisar la diferencia puntual que existe entre la evidencia digital con la evidencia electrónica. La evidencia digital es una prueba que tiene la forma de archivos digitales generados por propia voluntad de las personas como fotografías, documentos de Word, conversaciones, chats y otros muchos más, también son generadas con desconocimiento del usuario, como los metadatos o archivos logs. De otro lado, la evidencia electrónica tiene la particularidad que es física y a la vista. Pero lo que debemos subrayar es que ambas evidencias son significativas para una investigación.

Es pertinente precisar que las normas procesales en la actualidad no precisan el concepto de la evidencia digital. Con relación a ello diferentes organismos han definido el concepto, pero la que mejor se aproxima es el de la Organización Internacional de Evidencia Computacional, quienes señalan que es aquella información que se transmite a través de dispositivos digitales luego de haber sido creada y guardada que podría utilizarse en un proceso judicial. Considero que la particularidad como valor que tendría una evidencia digital seria que cada país regulara su legislación procesal que permitiera su utilización como evidencia recogida dentro del proceso. La evidencia digital respecto a su contenido pueden dividirse como registros que se producen en el dispositivo digital, como registros de eventos, transacciones o auditorias, también registros que no se generan sino que se almacenan en el dispositivo y los registros que si son generados por el usuario y se almacenan en el dispositivo. También se menciona que las evidencias digitales recogidas dentro de una investigación no solo son aquellas que se obtienen a mérito de un allanamiento o pericia, sino aquellas que se obtienen de los datos que se generan al conectarse a la red, como los tags, logs y metadatos.

No debemos dejar de lado lo relacionado con los principios de relevancia, confiabilidad y suficiencia, de la evidencia digital, de conformidad con el ISO/IEC 27037:2012, ya que estos principios son esenciales y exigentes para su admisibilidad en una investigación y proceso judicial. Si la evidencia no cumple con estas condiciones, serán consideradas irrelevantes y serán excluidas como elementos probatorios, por ello resulta importante validar su particularidad para mayor confiabilidad, debiendo ser auditada desde su obtención y ser verificada y demostrada, asimismo en lo que se refiere a su integridad se debe buscar que contenga los elementos idóneos que la sustenten y verifiquen mediante la participación de un perito informático.

Con relación a la volatilidad de la evidencia digital debemos precisar que es toda aquella

información que permanece temporalmente en el dispositivo y no volátil aquella información que se halla permanentemente en el dispositivo aun apagándose. Sumado a ello, es vital precisar las características de la evidencia digital en primer lugar no son visibles, tanto para las personas usuarias de las tecnologías sin conocimientos técnicos e inclusive los operadores de la justicia y policías. Así mismo, las evidencias digitales son frágiles y volátiles, debido a que son almacenadas en los dispositivos digitales y que al realizar una acción en ellas podría alterar su estado, por lo que resulta necesario constituir mecanismos particulares para protegerlas durante el procedimiento denominado cadena de custodia. Pueden ser alteradas o destruidas, sea por acción del usuario del dispositivo digital al copiarlo o grabarlo o por acción propia del sistema operativo instalado en el dispositivo que se está empleando. Son masivas, generando dificultad para ubicar información que se requiere en el proceso. Puede copiarse sin límite alguno, este procedimiento se efectúa técnicamente y con las herramientas adecuadas, se podrá clonar la información manteniendo la originalidad de sus características. Por otro lado, también es necesario indicar que con respecto a la recolección de la evidencia digital, esta debe ser admisible, para ser empleada en el proceso judicial. Debe ser auténtica y verdadera que se relacione indubitablemente con el hecho. Debe ser completa y suficiente que nos facilite tener una vista cabal respecto al hecho. Debe ser confiable, que su examen nos brinde seguridad de su autenticidad y debe ser creíble, entendible y convincente para los jueces.

Ante lo vertido la evidencia digital sin lugar a dudas ha generado como consecuencia un problema en cuanto al proceso penal respecto al nuevo medio de prueba en relación al medio de prueba tradicional, esto debido al uso de las tecnologías. En la actualidad el examen jurídico en relación a la evidencia digital resulta complejo y requiere del resguardo de garantías constitucionales que proporcione certeza como elemento probatorio. También estas nuevas evidencias denotan particularidades respecto a su manipulación a consecuencia del nivel de exhibición en la red y medios digitales operados por los usuarios, es por ello que la evidencia digital busca tener el valor legal de la información que incluye, para que sea validada en un proceso judicial, siendo indispensable para su admisión que la evidencia digital esté sujeta a procesos que permitan evaluar su fiabilidad, originalidad y aporte al proceso.

La evidencia digital en la actualidad viene siendo atendida procesalmente como si la acción se hubiera desarrollado en un espacio físico, generando consecuentemente evidencia física, habiéndose realizado el iter criminis dentro del ciberespacio, este tratamiento ha generado ciertos problemas. La evidencia digital advierte complejidades que deben tomarse muy en consideración, como el hecho de acceder a información personal, vulnerando los datos personales sensibles de las partes que no guardan relación con la investigación, abriendo el camino a futuras nulidades por excederse en los límites de respeto de sus derechos fundamentales, exponiendo de esta manera la evidencia obtenida. Los problemas que puede enfrentar la evidencia digital relacionan aspectos de su autenticidad, admisibilidad y legalidad que al no preservarse puede conllevar a su impertinencia y falta de valor probatorio por no acreditar credibilidad. Por ello resulta factible analizar adecuadamente la evidencia digital dentro de las formas de la razonabilidad, lógica y veracidad en el relato, para que sea creíble y contundente y no tenga dificultades de ser admitida dentro de un proceso judicial. Es así que el Convenio de Budapest recomienda pautas sobre las consideraciones a tener en cuenta con los medios de prueba, tales como el aseguramiento de datos, orden de presentación de datos, así como el registro y secuestro de datos.

Debemos considerar que la evidencia digital debe ser recogida, trasladada y custodiada correctamente para asegurar su legitimidad, cuidándola de no ser alterada y sea segura en su validez y eficacia en el proceso. Un aspecto fundamental también es que la evidencia digital ingrese correctamente al proceso sin ser condicionada por alguna rama del derecho. Asimismo, es importante apreciar cómo se enfrenta el proceso en el supuesto que la evidencia digital sea impugnada, de cómo la defensa técnica sepa debatir y argumentar para que el medio de prueba sea oportuna y valorada por el juez. Es por eso que es necesario que la prueba sea proporcionada

mediante un peritaje, siendo el perito competente para realizar su análisis, revisión y procedencia de la prueba, proporcionando al proceso información relevante que conduzca al juez a decisiones acertadas en la conclusión del proceso.

El proceso de recolección de la evidencia digital, nos presenta dos supuestos, el primero cuando la evidencia se halla dentro del territorio, donde la ley penal le alcanza y las investigaciones se pueden realizar sin inconvenientes. El segundo cuando la evidencia se halla fuera de la jurisdicción, para esta situación el arreglo procesal que lo prevé es el exhorto, para lo cual el juez que tiene a cargo el proceso debe requerir al juez del país en el cual se ubica la evidencia o se investiga el hecho su cooperación. Al respecto este procedimiento advierte una formalidad, situación que genera que los tiempos de atención sean largos o no se atiendan, presentándose también muchas veces que la recolección de la evidencia no sea eficaz y por consiguiente no se admita. Asimismo, en lo que se refiere a la localización de la evidencia hoy se presenta un nuevo problema que se denomina la nube, que se define como el lugar donde se guarda información en grandes volúmenes, de donde se accede a información que se aloja en equipos denominados servidores. Este tipo de situación tampoco se regula en los Códigos Procesales, debemos tener claro que al acceder a información en el ciberespacio a través de la red de Internet, este hecho nos redirecciona a determinado punto físico donde se ubica la información la cual se encuentra delimitada por una determinada jurisdicción, donde puede estar alojado el servidor. Por lo que al solicitar información debemos acudir prontamente a los convenios y cooperaciones internacionales para recabarla, el hacerlo de otra forma podría infringir el principio de territorialidad de ese país. El Convenio de Budapest es la norma internacional que mejor alternativas nos ofrece cuando hablamos de datos transfronterizos, en la actualidad muchos países ya se encuentran adheridos, incluyendo el Perú.

Debemos tener presente la necesidad que la evidencia digital sea, preservada, conservada y protegida en la cadena de custodia mediante un procedimiento pericial, para lo cual se hace muy necesario que los operadores de justicia y los policías sean capacitados para asegurar que estos procedimientos se ejecuten adecuadamente afín de asegurar el éxito de la admisibilidad de las evidencias digitales. Este procedimiento pericial se realizan a través de la informática forense, siendo que esta ciencia se encarga de ejecutar un conjunto de procedimientos y la aplicación de técnicas, para identificar, recolectar, extraer, preservar, documentar, presentando las evidencias digitales a fin de que sean aceptadas dentro de un proceso judicial. La informática forense sirve en la actualidad como soporte y gran ayuda a los jueces en diferentes procesos judiciales.

Otra de las acciones que servirían de forma eficaz para comprobar la integridad y autenticidad de la evidencia digital, es a través de la utilización de la herramienta denominada Hash, que es un algoritmo que nos permite tener la seguridad que las comunicaciones o archivos no se hayan alterado, se realiza mediante un examen generándose un registro en forma de cadena de caracteres antes y después de la comunicación de los datos, si estos son idénticos se interpreta que no han sido alterados. El Hash es la huella digital que imprime un archivo que nos permite verificar su integridad y autenticidad. También cuando los dispositivos digitales se comunican entre sí lo hacen a través de un protocolo de identificación denominado IP Protocolo de Internet, para conectarse los dispositivos entre sí, se identifican mediante los IP quienes cumplen la función de redirigir el tráfico de datos, es importante precisar que cada dispositivo que se conecta a Internet cuenta con una dirección IP. Adicionalmente, es importante las copias que se realizan a través de imágenes forenses informáticas, este procedimiento consiste en realizar una copia exacta que se realiza desde un dispositivo donde se almacena la información, realiza un proceso denominado copia bit a bit que duplica exactamente hacia un medio de almacenamiento distinto al del origen. Otras de las finalidades que tiene la imagen forense informática es buscar y obtener información relevante que podría haber sido borrada u ocultada y que sería empleada acertadamente en un proceso judicial. Y por último, es importante en los procesos considerar como valor probatorio de la evidencia digital los denominados metadatos que significan datos de los datos, información muy

útil, ya que describe detalladamente las características de cualquier tipo de archivo como cuando fue creado, cuando modificado, tipo de archivo, datos de geolocalización de imágenes y otros muchos más que son muy útiles para demostrar admisibilidad y confiabilidad.

Finalmente, la legislación comparada respecto al tratamiento de la evidencia digital de normas procesales, Panamá aplica el principio de libertad de medios probatorios, por lo que las evidencias digitales pueden ser aportadas y valoradas, debiéndose evaluarse previamente la fuerza probatoria como tal para tener la certeza de su confiabilidad e integridad y poder ser empleada dentro de un proceso judicial. En España la normatividad procesal enumera varios tipos de medios de prueba, tales como los documentos, medios de reproducción de imágenes y sonidos, entre otros, respecto a la evidencia digital, su admisibilidad la sostiene mediante teorías, entre ellas la denominada Teoría autónoma, que sustenta que la evidencia digital tiene una singular relación con la prueba documental, asimismo la Teoría analógica sostiene que las pruebas documentales y las digitales son de naturaleza equiparable y la Teoría de la equivalencia funcional sostiene que los documentos en soporte digital y soporte papel extienden identidad de efectos jurídicos. En Argentina los preceptos procesales equiparan la evidencia digital a la evidencia documental. En México la evidencia digital es aceptada en el derecho positivo, pero requiere previamente fiabilidad y seguridad de la forma como se generó el archivo y finalmente en Chile la evidencia digital será reconocida como tal si su probidad y factibilidad es demostrada, así como contar con fuerza probatoria bajo la forma de prueba documental para ser presentada dentro de un proceso judicial.

Consideraciones finales

De los resultados de estudio sistemático del presente trabajo denominado, la evidencia digital como medio de prueba en el Proceso Penal se concluye que:

La prueba para ser admitida requiere ser examinada y comprobada con el objeto con relación al hecho, así como las partes deben acceder y ser conducidos durante el procedimiento, materia de investigación, respetándose sus derechos fundamentales y el principio al debido proceso. La evidencia digital, al no haber sido regulada en la legislación procesal, se incorpora mediante el principio de la libertad probatoria, siendo su fundamento la analogía, el mismo que faculta el empleo de un medio de prueba legal, sin transgredir garantías y derechos de las personas y las facultades de los sujetos procesales.

La evidencia digital es medio de prueba en forma de archivo digital, el cual se produce con voluntad por el usuario o sin conocimiento de él, al ser generadas por el sistema operativo; por otro lado, la evidencia electrónica se distingue de la evidencia digital, ya que la primera tiene la particularidad que es física, visual y la segunda la forma de archivos binarios, pero ambas evidencias son significativas para la investigación. La evidencia digital en lo que se refiere a su contenido es aquella que se produce en el dispositivo digital, como eventos, transacciones o auditorias, y los registros generados por el usuario, ambas se almacenan en el dispositivo. También son aquellas que se obtienen al conectarse a la red, como los tags, logs y metadatos.

Los principios de relevancia, confiabilidad y suficiencia, de la evidencia digital, son esenciales para su admisibilidad en una investigación y proceso judicial, tal como se establece en el ISO/IEC 27037:2012. Las características de la evidencia digital se distinguen como no visibles, son frágiles y volátiles, pueden ser alteradas o destruidas, son masivas y pueden copiarse sin límite alguno. Respecto a su recolección, debe ser admisible, ser auténtica y verdadera, completa y suficiente, y debe ser confiable. Si la evidencia no cumple con estas condiciones expuestas, serán consideradas irrelevantes y serán excluidas.

La evidencia digital es atendida como si la acción se hubiera desarrollado en un espacio físico y no en el ciberespacio. También se advierte que al obtener y acceder a información personal del

investigado se vulnera sus datos personales sensibles que no guardan relación con la investigación, conllevando a nulidades al no respetar de sus derechos fundamentales. Del análisis de la legislación procesal comparada, del tratamiento de la evidencia digital en países de Europa y Latinoamérica, se concluye que la evidencia digital es considerada como prueba documental, debiéndose evaluar su fuerza probatoria para tener la certeza de su confiabilidad e integridad y poder ser empleada dentro de un proceso judicial.

La evidencia digital debe ser recogida, trasladada y custodiada para asegurar su legitimidad, por ello es necesario que sea obtenida mediante la pericia informática forense, por lo que se requiere que los operadores de justicia y los cuerpos de policía, consideren su importancia y valor, debiendo ser capacitados sobre estos procedimientos para asegurar su correcta ejecución y la admisibilidad de la evidencia digital. En el proceso de recolección de la evidencia digital, si se encuentra dentro del territorio, la ley penal le alcanzará, pero cuando se halla fuera de la jurisdicción, el arreglo procesal será el exhorto, para lo cual deberá requerirse al juez del país donde se ubica la evidencia, su cooperación. Este hecho aplaza los tiempos de atención y respuesta o en el peor de los casos no se logra atender.

Es necesario comprobar la integridad y autenticidad de la evidencia digital, para ello debe emplearse herramientas como el Hash, algoritmo que permite verificar que los archivos no se hayan alterado respecto a su origen, asimismo la importancia del protocolo de identificación y comunicación denominado IP Protocolo de Internet, que nos permite conocer con qué dispositivo se conecta y su tráfico de datos. También saber la función que cumple la copia de imágenes forenses informáticas que permite realizar una copia exacta desde un dispositivo a otro. Y por último, es importante conocer el valor de los metadatos que significan datos de los datos, información detallada que describe las características de cualquier tipo de archivo.

Referencias

Alfonso, S. (2021). La prueba electrónica en el proceso penal. (Tesis para optar el Grado de Maestro). Universidad de la Laguna. Recuperado de: https://bit.ly/3FWWbFN

Cenci, M. (2021). Los desafíos penales de la evidencia digital. (Tesis para optar el grado de bachiller). Universidad Nacional del Comahue. Recuperado de http://rdi.uncoma.edu.ar/handle/uncomaid/16652

Del Valle, D. (2018). Evidencia Digital. Universidad Empresarial Siglo 21. Recuperado de: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/16396/LOPEZ%20DANIELA%20DEL%20VALLE.pdf?sequence=1

Espinoza, V. (2021). Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima. Universidad Cesar Vallejo. Recuperado de: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/90185/Espinoza_PV-SD.pdf?sequence=1

Estupiñan, T., Mora, K., y Santiago, C. (2019). Importancia de la Memoria como Evidencia Digital en la Informática Forense. Actas de la Multiconferencia internacional LACCEI de Ingeniería, Educación y Tecnología 2019-julio. Recuperado de: http://www.laccei.org/LACCEI2019-MontegoBay/full_papers/FP479.pdf

Gómez, D., Acevedo, J., y Aguirre, J. (2021). Autenticidad y debido proceso en los mensajes de

WhatsApp: Una revisión en los casos de divorcio. Revista chilena de derecho y tecnología, 10(2), 123-148. Recuperado de: https://dx.doi.org/10.5354/0719-2584.2021.58039

Herrera, J. (2021). Estudio de la prueba electrónica, su preservación, adulteración, mecanismos de defensa y valoración en el proceso judicial. Universidad Externado de Colombia. Recuperado de https://bdigital.uexternado.edu.co/handle/001/3948

Jiménez, W. G. y Meneses, O. (2017). Derecho e Internet: introducción a un campo emergente para la investigación y práctica jurídicas. Revista Prolegómenos Derechos y Valores, 20, 40, 43-61. DOI: http://dx.doi.org/10.18359/prole.3040

Muhammet, A., Morina, M., y Papajorgji, E. (2021). Digital Evidence and Prohibitions of Evidence Evaluation. Journal of Educational and Social Research, 11(5), 67. Recuperado de: https://doi.org/10.36941/jesr-2021-0106

M. Rodrigo, F. (2021). La prueba digital en el proceso penal y la preservación de los derechos fundamentales. *Revista Académica Escola Superior do Ministério Público do Ceará* , *13* (1), 135–161. https://doi.org/10.54275/raesmpce.v13i1.154

Molina, C., Beltrán, L., y Contreras, O. (2021). La Prueba Electrónica y Digital Aclaración de las diferencias jurídicas en Colombia. Institución Universitaria Politécnico Gran colombiano. Recuperado de: http://hdl.handle.net/10823/2147

Naula, D., N., Quevedo, R., y Zamora, A. (2022). El protocolo de reconocimiento de medios digitales frente a la inobservancia del debido proceso penal. Revista polo del conocimiento, 7(6), 229-248.Recuperado de: https://polodelconocimiento.com/ojs/index.php/es/article/view/4071

Ochoa, P. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. Revista Economía y Política, (28), 35-44. Recuperado de: https://doi.org/10.25097/rep.n28.2018.03

Palomo, L. E., y Guillet, S. M. (2021). Evidencia digital de la nube. el aporte probatorio en Santiago del Estero. *Difusiones*, *21*(21), 59–75. Recuperado a partir de http://revistas.ucse.edu.ar/ojsucse/index.php/difusiones/article/view/394

Parra-Sichaca, D. (2019). Requisitos jurídicos para la validez jurídica de la prueba digital. (Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. Recuperado de: https://hdl.handle.net/10983/23853

Piccirilli, M. (2019). Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos: legislación vigente, anteproyectos y Convenio de Budapest (trabajo final de especialización). Universidad de Buenos Aires. Recuperado de: http://repositoriouba.sisbi.uba.ar/gsdl/cgi-

bin/library.cgi?a=d&c=adrespe&cl=CL1&d=HWA_6501

Prayudi, Y., Ashari, A., y Priyambodo, T. (2020). The Framework to Support the Digital Evidence Handling: A Case Study of Procedures for the Management of Evidence in Indonesia. Journal of Cases on Information Technology (JCIT), 22(3), 51-71. Recuperado de: http://doi.org/10.4018/JCIT.2020070104

Rivero, L. (2017). Delitos informáticos y la evidencia digital en el proceso penal peruano en el 2017. Universidad Cesar Vallejo. Recuperado de: https://hdl.handle.net/20.500.12692/23302

Samonova, V. (2022). Electronic Evidence in Administrative Proceedings. Cuestiones Políticas, 40(73), 726–740. Recuperado de: https://doi.org/10.46398/cuestpol.4073.4

Silva, G. (2021). La obtención de la prueba digital en los delitos informáticos en el distrito fiscal de Lima Norte, 2021. Universidad Cesar Vallejo. Recuperado de: https://hdl.handle.net/20.500.12692/96824

Schirakian, N. (2021). Evidencia informática: ¿un nuevo paradigma para el derecho procesal penal? Universidad de San Andrés. Recuperado de: http://hdl.handle.net/10908/18968