Revista de la Maestría en
DERECHO PROCESAL
RMDPro

Prueba digital y cibercriminalidad: una mirada a los principios de libertad probatoria, inmediación y contradicción*

Digital Evidence and Cybercrime: A Perspective on the Principles of Free Assessment of Evidence, Immediacy and Adversarial Proceedings

Raquel Limay Chavez
Doctoranda y miembro de la Cátedra de Cultura Jurídica de la Universidad de Girona (España).
Código ORCID: 0000-0001-9278-1067 | Contacto: raquel.limayc@udg.edu

Resumen

La presente investigación busca aportar al estudio y análisis general de las denominadas «pruebas digitales» generadas en el marco de hechos delictivos vinculados al fenómeno de la cibercriminalidad. Este propósito reviste especial relevancia ante la creciente preocupación de los Estados y de los sistemas de justicia por combatir las actividades ilícitas que se desarrollan en el ciberespacio. El trabajo se centra en el examen de tres principios procesales y probatorios —libertad probatoria, inmediación y contradicción— con el objetivo de fortalecer la comprensión del proceso penal a la luz de la nueva realidad digital y tecnológica, la cual exige replantear los enfoques tradicionales sobre los principios y valores que rigen nuestros sistemas judiciales.

Palabras clave: Cibercriminalidad, prueba digital, inmediación, contradicción, libertad probatoria.

* La presente investigación ha sido realizada en el marco de la financiación que me fue concedida tras la resolución favorable de la Convocatoria Extraordinaria de Ayudas 2025 de la Fundación Privada Manuel Serra Domínguez (Barcelona, España), obtenida en julio de 2025, destinada al apoyo de proyectos de investigación vinculados a los fines de la Fundación.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

Abstract:

This research aims to contribute to the study and analysis of so-called "digital evidence" produced in the context of criminal acts linked to the phenomenon of cybercrime. This objective is particularly relevant in light of the growing concern of States and justice systems regarding the fight against illicit activities carried out in or through cyberspace. The project focuses on examining three procedural and evidentiary principles—free assessment of evidence, immediacy, and adversarial proceedings. The purpose is to strengthen the understanding of criminal procedure in view of the new digital and technological reality, which demands a reconsideration of the traditional approaches to the principles and values that underpin our current judicial systems.

Keywords: *Cybercrime, digital evidence, immediacy, adversarial proceedings, free assessment of evidence.*

Recibido: 25 de agosto de 2025 | Aprobado: 1 de diciembre de 2025

1. Introducción

Nuestros procesos penales están diseñados con un gran protagonismo de las pruebas tradicionales, como las pruebas testimonial, documental y pericial pensadas en un contexto de averiguación de la verdad o esclarecimiento de los hechos que tienen lugar en la realidad; esto es, el espacio físico y perceptible. La doctrina civilista clásica estudió el impacto, desarrollo y apreciación de dichas pruebas también en un escenario físico, tangible, visible y perceptible. Actualmente, los procesos penales por criminalidad se han expandido vertiginosamente abarcando inclusive espacios que trascienden lo tangible; así, tienen lugar en un escenario o un entorno digital que ha sido denominado el «ciberespacio». En este se cometen cibercrímenes o delitos informáticos cuyo impacto y ejecución transgrede y, a la vez, emplea las tecnologías de la información y comunicación.

Se trata de una era donde reinan la tecnología y la virtualidad como medio y fin para la comisión de ilícitos.

El nuevo escenario de cibercriminalidad sugiere que repensemos un proceso penal, reglas procedimentales y probatorias, principios y garantías que fueron estudiadas desde la doctrina procesal, pero en un contexto procesal de delincuencia tradicional[1]. Parece sumamente relevante prestar atención a los nuevos cambios que pueden significar repensar los actuales principios del proceso. En este sentido, al ser la presente investigación un análisis que tiene como base los estudios de la prueba, abordaré concretamente tres principios que tienen importancia vital para el proceso penal: los de libertad probatoria, inmediación y contradicción.

En la primera sección se abordará la noción y conceptualización de la cibercriminalidad en el ámbito del proceso penal, analizando las formas y herramientas actuales para su investigación, procesamiento y enjuiciamiento, además de precisar qué tipos de pruebas se emplean para esclarecerlos. Seguidamente, el segundo apartado está dirigido al análisis de las pruebas digitales, evaluando sus principales notas características, además de presentar el estado de la cuestión sobre la forma de procesamiento y abordaje de este medio de prueba digital, identificando sus problemas en la actividad probatoria[2]. Finalmente, el último apartado está dirigido a evaluar la actividad probatoria a la luz de los principios del proceso de libertad probatoria, de inmediación y de contradicción (Consejo de la Unión Europea, 2016).

2. El nuevo escenario de la cibercriminalidad

Como bien lo ha identificado el Consejo de la Unión Europea (2024), la ciberdelincuencia adopta diversas formas y el ámbito cibernético facilita numerosos

1 La delincuencia tradicional y las pruebas tradicionales deben ser comprendidas, desde mi perspectiva, como aquellas que no hacen uso de medios tecnológicos o que se desarrollen en espacios virtuales.

2 No debe dejar de mencionarse que la doctrina ha elaborado propuestas para apreciar la prueba digital; así, por ejemplo, Arbós i Llobet (2011). En dicho libro, Xavier Abel Lluch indica que el análisis de la prueba electrónica se estructuraría sobre los siguientes elementos: el soporte, que sería magnético u óptico (CD, USB, *flash drive*); y el contenido, que podría separarse del soporte, contiene una estructura lógica constituida por el *software* y el *hardware* perceptibles a los sentidos que podría ser analizada. Asimismo, la firma y la fecha que se encuentran grabadas en el dispositivo y en certificaciones digitales (firma digital) otorgarían mayor seguridad al documento (2011, pp. 37 y ss.).

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

delitos comunes y surgidos del entorno digital. Entre las acciones delictivas se encuentran, por ejemplo, hacerse con el control de dispositivos personales usando programas maliciosos, robar o poner en peligro datos personales y derechos de propiedad intelectual para cometer fraudes en línea, utilizar internet y las plataformas de redes sociales para distribuir contenidos ilícitos, y usar la *dark web* para vender bienes ilícitos y servicios de piratería informática. Precisamente, en aras de esclarecer la comisión y sancionar los ilícitos que forman parte de la ciberdelincuencia se emplean diversas pruebas, tanto para averiguar los hechos delictivos en una decisión final como para emplearlas durante el procedimiento con el fin de, por ejemplo, aplicar medidas de coerción o restrictivas.

La vulneración y ataques a los datos e información privada y pública cometidas a través de los llamados ciberdelitos, que emplean tecnologías de la información y comunicación, así como su utilización para los ataques a la ciberseguridad, seguridad pública y privada, vienen socavando la democracia y la confianza en los actuales procesos judiciales para enfrentar estas nuevas formas de criminalidad, que definitivamente generan un desmedro para la seguridad del Estado y de sus instituciones.

Así, en un Estado constitucional de derecho las decisiones deben tomarse de formas democráticas que respondan a la verdad de lo ocurrido. Lo que sucede con la ciberdelincuencia es que estas son prácticas delictivas antidemocráticas que socavan diversos bienes valiosos en la sociedad, como la intimidad, la comunicación, el patrimonio y los datos personales, entre otros[3]. Precisamente, para evitar un contexto en el que circule información digital que afecte derechos individuales y colectivos, se requiere asumir una posición clara de enfrentamiento a las nuevas formas y métodos sofisticados de criminalidad.

En ese marco, para salvaguardar el correcto desarrollo de los procesos judiciales, corresponde que las decisiones sean lo más cercanas a la verdad; por ello, debe procurarse que la prueba digital recolectada e introducida al proceso sea fiable, lo que permite que las decisiones se condigan en la mayor medida posible con el esclarecimiento de los ciberdelitos. Las investigaciones y postulaciones previas de los procesos deben contar con herramientas procesales actuales que permitan lograr esta finalidad, pero antes es importante delimitar el nuevo contexto o esquema de los procesos por cibercriminalidad.

3 De acuerdo con el análisis del impacto económico y científico de la investigación desarrollada por el Consejo de la Unión Europea (2024), «las formas de ciberdelincuencia, como la explotación sexual de menores en línea, causan graves daños a sus víctimas y significa un total de 5,5 billones, que es el coste anual mundial de la ciberdelincuencia».

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

De ahí que se haya identificado que la ciberdelincuencia afecta, entre otros ámbitos, a los procesos de formulación de políticas públicas, debates sociales y decisiones importantes en los ámbitos de la administración de justicia, afectando además la seguridad jurídica, así como los recursos económicos del Estado otorgados para la adecuada impartición de la justicia por los órganos jurisdiccionales y de investigación. Por consiguiente, existe la imperiosa necesidad de que las partes procesales, así como el órgano jurisdiccional, conozcan en cierta medida el funcionamiento de las ciencias y tecnologías para enfrentar adecuadamente la expansión de delitos que se desenvuelven en el ciberespacio. Como bien lo indica la Comunicación de la Comisión al Parlamento Europeo (2018): «la desinformación puede mermar la confianza en la ciencia y en las pruebas empíricas», lo que evidentemente dificulta una adecuada apreciación y desarrollo de la actividad probatoria[4].

Es previsible que, si no se fortalecen nuestros sistemas de justicia y la forma de afrontar la criminalidad, los ciberataques aumenten, lo que generaría en definitiva que tanto los datos personales como la economía de los miembros de la sociedad se encuentren más vulnerables a las ciberamenazas y los ciberataques. Estos sobrepasan los sistemas de ciberseguridad que vienen desarrollándose y merman sectores vitales de la sociedad, incluyendo los de la administración de justicia, las comunicaciones y las finanzas, que se han visto cada año más influenciados por el uso y aplicación de tecnologías digitales que intervienen en actividades esenciales.

Como bien lo ha referido el Consejo de Europa, «los ciberataques y la ciberdelincuencia están aumentando en toda Europa, y cada vez son más sofisticados. Esta tendencia seguirá agravándose en el futuro» (Consejo de la Unión Europea, 2024)[5]. Por ello, se requiere proponer desde todos los ámbitos, incluyendo el jurídico, que exista una respuesta firme en materia de ciberseguridad que permita «crear un ciberespacio abierto y seguro, que podrá generar entre los ciudadanos una mayor confianza en las herramientas y servicios digitales» (Consejo de la Unión Europea, 2024).

---

4 Sobre la rapidez de transmisión de la información, el informe *Outlook on the Global Agenda 2014* resaltó: «It's also imperative to highlight the volume and rapid dissemination of online misinformation. When you are dealing with social media, you are dealing with big data» (World Economic Forum, 2014, p. 29b).

5 Por ejemplo, se sostiene «que 41 000 millones de dispositivos en todo el mundo estarán conectados a la internet de las cosas de aquí a 2025».

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

Se requiere de una propuesta de cara a las modalidades de crimen que refuerce la actividad de obtención de pruebas digitales fiables que sirvan para esclarecer los hechos delictivos, pero además se necesita de una actividad probatoria robusta y, en general, de un sistema procesal penal que afronte los daños sociales, económicos, judiciales y políticos que genera esta forma de criminalidad[6].

Ahora bien, ya expuesto un marco general sobre el contexto de la expansión de la cibercriminalidad, se continuará con el desarrollo de las pruebas digitales en la ciberdelincuencia.

3. El contexto de las pruebas digitales y los ciberdelitos

El profesor Serra Domínguez refería que «el análisis de la prueba no es exclusivamente jurídico, sino también es una actividad humana, que es usada en el ámbito del derecho» (Serra Domínguez, 2023, p. 2323); y, en efecto, al hablar de prueba abordamos un concepto dinámico y siempre en evolución que sobrepasa el ámbito jurídico, pero que igualmente tiene impacto en él. En ese sentido, la presencia de la prueba electrónica, digital o tecnológica[7] es una realidad manifiesta en la actual era de la digitalización. Se viene utilizando cada vez con mayor frecuencia en los procesos judiciales penales, civiles, laborales y de cualquier naturaleza. Además, su incidencia, lejos de ser insignificante, ha ganado espacio en la toma de decisiones judiciales como medio de prueba decisivo, único o, en todo caso, corroborantes del esclarecimiento de los hechos materia de probanza.

El empleo y la notoria presencia de las pruebas digitales se contrasta, sin embargo, con el actual sistema procesal, donde las construcciones normativas, los principios del proceso y el tratamiento probatorio que regulan su valoración y actividad probatoria están pensados para medios de prueba tradicionales como

6 Estrategias de seguridad de la Unión Europea: «Los ministros de la UE fijaron como objetivo clave lograr la autonomía estratégica preservando al mismo tiempo una economía abierta, para lo cual es necesario aumentar la capacidad de adoptar decisiones autónomas en el ámbito de la ciberseguridad con el fin de reforzar el liderazgo digital y las capacidades estratégicas de la UE» (Consejo de la Unión Europea, 2021).

7 No es menos importante la denominación de las llamadas «pruebas que emplean la tecnología», pero este trabajo se centrará concretamente en sus problemas más que en el empleo de su denominación.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

la prueba testimonial y documental[8-9]. Así, cuando revisamos los escritos sobre prueba de Serra Domínguez, se aprecia que considera como un catálogo de pruebas casi cerrado a la testimonial, la documental, la confesión, la inspección ocular y el reconocimiento judicial (p. 2324). Actualmente, esta concepción amerita una interpretación actualizada.

Es necesaria una adecuada actividad probatoria durante la obtención, admisión y valoración de pruebas digitales o electrónicas en aras de desarrollar mejores procesos judiciales que esclarezcan la comisión de ciberdelitos. También es relevante conocer los hechos delictivos cometidos por sujetos activos que se valen de información, datos privados y públicos, bienes colectivos e individuales, de alcance nacional e internacional, obtenidos o producidos por medios tecnológicos. El alcance delictivo se ha extendido vertiginosamente, es por ello que el Consejo de la Unión Europea (2024) ha señalado que «La UE está trabajando en varios frentes para promover la ciberresiliencia, luchar contra la ciberdelincuencia e impulsar la diplomacia y la defensa».

Uno de los ámbitos en los que se requiere del empleo de la prueba digital es definitivamente en aquellos procesos penales donde se pretende esclarecer la comisión de delitos informáticos, ciberdelitos o cibercrímenes[10]. Los ciberdelitos se presentan como consecuencia de la expansión relativamente reciente de la ciberdelincuencia o cibercriminalidad consistente en aquellos ilícitos cometidos a través de medios tecnológicos e informáticos para la creación, difusión, interceptación de datos o información privada, que además de perjudicar la intimidad,

8 Cabe precisar que, en algunas legislaciones, las fuentes de índole electrónica, digital o tecnológica han sido introducidas al proceso judicial a través de los medios de prueba documental. Actualmente, con el empleo de las nuevas tecnologías, dada la situación de preeminencia de la virtualidad en la cual se encuentran nuestros procesos penales, es recurrente el reemplazo del uso del documento en papel por el documento virtual, lo que amerita en definitiva un cambio en su regulación.

9 En el comunicado emitido por la Comisión Europea en Bruselas el 17 de abril de 2018, se advierte la preocupación por los actuales mecanismos legales y procesales de lucha contra la cibercriminalidad. Este sostuvo que: «Las autoridades encargadas del cumplimiento de la ley siguen trabajando con métodos complicados, mientras que los delincuentes recurren a tecnologías rápidas y de vanguardia. Debemos dotar a esas autoridades de métodos del siglo XXI para luchar contra la delincuencia, al igual que los delincuentes utilizan métodos del siglo XXI para cometer sus delitos, no podemos permitir que los delincuentes y los terroristas exploten las tecnologías de la comunicación electrónicas y modernas para ocultar sus actividades delictivas y eludir la acción de la justicia».

10 No se abordará la diferencia entre los términos empleados, aunque haya sido materia de un serio estudio para clasificarlas (Elías, 2025, p. 54); en cambio, sí se usarán estas denominaciones para referir a la delincuencia que emplea las tecnologías de la información y la comunicación.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

puede dañar bienes jurídicos valiosos como la indemnidad sexual, el orden financiero y el secreto de las comunicaciones, entre otros.

Así, por ejemplo, el preámbulo del Convenio de Budapest del 23 de noviembre de 2001 abordó los problemas relativos a la ciberdelincuencia, considerando la tipificación de diversos tipos penales al ser necesaria para «prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de estos, garantizando la tipificación como delito de dichos actos».

De manera más específica, la doctrina propone la clasificación entre delitos informáticos en sentido amplio, lo que comprende la afectación a bienes jurídicos clásicos, pero empleando medios tecnológicos. Por ello, también se les conoce como «ciberdelitos réplicas» (Miró, 2012, p. 51) y «ciberdelitos en sentido estricto» o «puros», estos últimos referidos a aquellas conductas que, de manera directa o indirecta, lesionan o ponen en peligro la confiabilidad, integridad o disponibilidad de datos y sistemas informáticos (propiamente, los ciberdelitos), utilizando también los medios virtuales (Miró, 2012, p. 52; Requejo, 2023, p. 29). Sin duda, la comisión de estos delitos son manifestaciones de un cambio en el panorama delictivo que se vale de las nuevas tendencias tecnológicas, haciendo del entorno virtual un nuevo escenario criminal.

La cibercriminalidad supone un ataque directo a derechos fundamentales y bienes jurídicos valiosos para nuestros procesos y sistemas judiciales. Estos mellan los mecanismos y herramientas generadas por las políticas de ciberseguridad en la protección de datos personales y de nuestras comunicaciones, así como de diversos derechos relacionados con el secreto de las comunicaciones, la intimidad personal y la indemnidad de las personas, muy frecuentemente en desmedro del patrimonio o contra el orden financiero, que tiene como principal característica la transnacionalidad. Como bien lo afirma la ONU (2021): «Los avances tecnológicos están convirtiendo simples delitos en amenazas mundiales». Debido a esta razón, un sector doctrinario importante expone la necesidad de regular los ciberdelitos que han ido expandiéndose y abarcando modalidades y formas de ejecución diferentes de la delincuencia tradicional.

Precisamente, en aras de esclarecer la comisión, ejecución y sancionar los ilícitos que conforman el fenómeno de la ciberdelincuencia, durante la investigación se busca recopilar diversas pruebas digitales y tradicionales[11] que sirven

11 Se empleará este término para abordar las pruebas que no emplean tecnologías de la información y comunicación.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

de fundamento para requerir medidas de coerción restrictivas, limitativas o para, finalmente, decidir condenas o absoluciones de cibercrímenes, siempre teniendo como base las pruebas digitales. Como bien refiere Armenta Deu (2018), «los medios tecnológicos son fuente esencial de diversas investigaciones» (p. 68); su incorporación al proceso es necesaria y actualmente recurrente. Así, por ejemplo, durante el proceso, la prueba digital es empleada desde las fases iniciales de investigación preliminar y preparatoria cuando se trata de recabar correspondencia electrónica por razón de una interceptación o incautación postal, elementos que pueden ser determinantes para requerir medidas limitativas de derechos; o cuando se emplean documentos obtenidos por dispositivos como celulares, *tablets* y USB, entre otros, que son introducidos y valorados como prueba trascendental para sustentar una condena o absolución[12].

En la misma línea, Ortiz sostiene que «utilizar cualesquiera medidas tecnológicas de investigación destinadas a obtener información en formato digital se antoja un pilar esencial en cualquier investigación en la actual sociedad informatizada en la que vivimos» (Ortíz, 2013, p. 7). Así, la prueba digital es producida por los sistemas digitales o informáticos; se crea, almacena y reproduce en estos mismos, a los cuales es posible acceder a través de los medios o aparatos tecnológicos que actualmente son ingresados al proceso a través de la prueba documental, en tanto no existe una regulación normativa específica en muchas legislaciones sobre el uso de pruebas digitales.

Ahora bien, si realizamos una comparación entre las pruebas tradicionales y las pruebas digitales, la doctrina ha sido conteste en señalar que estas «son frágiles y pueden alterarse, dañarse o destruirse si se tratan o examinan de un

12 Por ejemplo, en el R. N. N.º 222-2019 la Corte Suprema del Perú declaró que no había nulidad en la condena de un imputado por el delito de ofensas al pudor —exhibiciones y publicaciones obscenas— y otro en agravio de una menor de edad. En este extremo de los hechos, se le imputó al acusado haber enviado a la menor, vía WhatsApp, imágenes y contenido (fotos de su órgano sexual y de personas adultas manteniendo relaciones sexuales —entre ellas, de él y su conviviente, que era la hermana de la menor—, así como de mujeres adultas desnudas) con el propósito de que la menor le enviara fotos desnuda, pues ya había logrado que le mandara imágenes de sus nalgas. Este hecho fue descubierto por la madre de la menor agraviada el 2 de diciembre de 2017, tras revisar el celular de esta. Además, encontró conversaciones de similar contenido, lo que motivó la inmediata denuncia después de que la menor le contara sobre las acciones realizadas por el imputado. El acusado recurrió indicando una indebida valoración sobre la conversación sostenida con la menor agraviada, consignada en el acta de visualización y captura de los mensajes vía WhatsApp del teléfono celular. Sin embargo, la Sala Penal Permanente (Recurso de Nulidad N.° 222-2019/Lima, 2019), luego de evaluar esta prueba electrónica, así como las testimoniales recogidas en cámara Gesell y pericial, determinó su responsabilidad.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

modo inadecuado» (Oficina de las Naciones Unidas contra la Droga y el Delito, s.f.). Si bien los actuales sistemas de justicia han implementado mecanismos para «incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como obtener pruebas electrónicas de los delitos» (Convenio de Budapest, 2001), aún persiste el riesgo y el empleo de redes y sistemas informáticos, telemáticos y cibernéticos que son muy adecuados para cometer y ocultar delitos, especialmente con el avance constante y sofisticación de la tecnología a la que tiene acceso la mayoría de la población mundial[13].

El esclarecimiento de los hechos delictivos en contextos de cibercriminalidad depende, entre otros medios probatorios, de la recopilación de pruebas digitales que buscan definir los hechos que se han producido en un escenario delictivo de índole virtual y, de ser estos establecidos, que puedan ser sancionados debidamente. Sin embargo, problemas concretos relacionados con sus características de fragilidad y manipulación de las pruebas digitales pueden incidir en la dificultad de obtenerlas y preservar su fiabilidad; por ejemplo, porque los entornos digitales se encuentran desprovistos de barreras y límites en su uso, lo que dificulta su obtención y posterior valoración.

De ahí que Taruffo (2008), a través de sus textos, haya advertido hace más de dos décadas atrás que

> el problema de controlar la fiabilidad de las pruebas informáticas se resuelve exigiendo la prueba de diversas condiciones, al menos cuando la autenticidad o la fiabilidad de las pruebas informáticas se impugne; el equipo de cómputo debe ser estándar, el proceso tiene que haber sido ejecutado de manera correcta, y el programa haber sido puesto en marcha adecuadamente. En pocas palabras: se debe probar que toda la maquinaria que produjo el archivo funcionó correcta y apropiadamente (pp. 86-87)[14].

Dada la relevancia de las pruebas digitales, resulta necesario repensar el procesamiento de delitos cometidos en el ciberespacio por cuanto es claro que

13 De acuerdo con el Departamento de Asuntos Económicos y Sociales de la ONU (2015), «en la actualidad más del 80% de los hogares en los países desarrollados tiene acceso a Internet, mientras que dos tercios de los países en desarrollo no lo tienen. Las mujeres son la mitad de la población mundial, sin embargo 200 millones de ellas tienen menos acceso a la red que los hombres. Hay que superar estas brechas».

14 Claro que estos criterios en la actualidad serían superables, puesto que la vulneración en ámbitos de cibercriminalidad ha superado modos tradicionales de ataque a los sistemas *software* o tangibles de un ordenador.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

la cibercriminalidad, al emplear un conocimiento tecnológico especializado, no merece el mismo tratamiento de aquellos delitos cometidos en el mundo real, que responden a una criminalidad tradicional; en tanto que las medidas aplicables, así como la actividad probatoria, revisten una complejidad que no puede ser comparada a la forma predominante de cibercriminalidad.

4. La actividad probatoria de la prueba digital en la cibercriminalidad

La criminalidad común ha evolucionado atacando espacios (ciberespacios) que, como se ha mencionado antes, se encuentran en muchas ocasiones fuera del alcance de las herramientas y procesos judiciales actuales. La administración de justicia y el sistema judicial no han evolucionado a la misma velocidad que las diversas formas y modalidades de criminalidad. A pesar de ello, el ingreso de medios de prueba digitales a nuestros sistemas de justicia se torna más frecuente, precisamente, por la facilidad de obtener la información en redes informáticas, la cual contrasta con los mínimos o nulos controles aplicados para detectar su fiabilidad, lo que puede terminar por socavar la institucionalidad del sistema de justicia en el marco de un Estado constitucional de derecho (Sanjurjo, 2020, pp. 199-200).

Una indebida actividad probatoria de la prueba digital en el escenario de la cibercriminalidad, como manifestación de ataques a la ciberseguridad, afecta de forma sistemática diversos contextos de nuestra sociedad actual, los derechos humanos y la democracia de nuestros países. Como lo ha mencionado el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Ciberseguridad (2019):

> La intensificación de la digitalización y de la conectividad trae consigo un aumento de los riesgos en materia de ciberseguridad, con lo que la sociedad en general resulta más vulnerable a las ciberamenazas y se exacerban los peligros a que se enfrentan las personas, incluidas las personas vulnerables. A fin de atenuar dichos riesgos, es preciso adoptar todas las medidas necesarias para mejorar la ciberseguridad.

En el contexto de los procedimientos judiciales por cibercriminalidad, la actividad de investigación y conformación, así como la admisión y valoración de los medios de prueba digital, son vitales para lograr un recorrido por el procedimiento probatorio óptimo que permita esclarecer determinados ciberdelitos que

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

menoscaban la ciberseguridad[15]. Las pruebas digitales pueden ser tan frágiles y manipulables que, llegado el momento de valorarlas, pueden adolecer de alguna contaminación que no fue evitada en la fase de investigación y que finalmente impactará en el debido esclarecimiento de los hechos.

Debe apuntarse a que la prueba sea recabada con todas las medidas de custodia, que sea admitida de acuerdo con los criterios de relevancia, y que sea actuada y valorada de manera objetiva, atendiendo a los diversos problemas probatorios que derivan de sus características intrínsecas. De esa manera, se procura optimizar los procesos penales judiciales, especialmente en este tipo de delitos, que dependen de la adecuada apreciación y conocimiento de las nuevas tecnologías.

Atendiendo al impacto en la actualidad, los procesos judiciales no son ajenos a las TIC (tecnologías de información y comunicación). Por ello, resulta necesario e imprescindible construir un sistema de investigación, admisión y valoración de pruebas que haga uso de estas herramientas tecnológicas proporcionadas por la ciencia, en aras de obtener pruebas digitales fiables que faciliten el esclarecimiento de delitos graves como los ataques informáticos, cibercrímenes que atacan los datos e información personal que circula en la red y el entorno virtual, y que además de la reserva de datos personales y públicos, afectan a bienes jurídicos preciados como la intimidad e indemnidad personal, y muy especialmente el patrimonio y orden financiero.

En ese sentido, la construcción racional de la actividad probatoria de conformación, práctica y valoración de las pruebas digitales en los procesos penales por ciberdelitos amerita una adecuada recopilación y apreciación judicial de estos medios probatorios en los actuales procesos penales por cibercriminalidad. La atención a la actividad probatoria permitirá que, una vez tenida la noticia criminal en este tipo de procesos, se puedan identificar a través de pruebas digitales los ataques a los sistemas de seguridad en el ciberespacio, de tal modo que se aclaren y sancionen los diversos ilícitos penales que emplean conocimientos tecnológicos y especializados.

15 De acuerdo con el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación: la ciberseguridad incluye las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de dichos sistemas y de otras personas afectadas por las ciberamenazas.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

4.1. Problemas en la actividad probatoria

Durante el desarrollo de todo el procedimiento probatorio, las pruebas digitales pueden adolecer de diversos problemas. Así, por ejemplo, podrían estar basadas en información proveniente de fuentes no confiables que brinden datos erróneos de forma intencional o, por otro lado, de fuentes de información que no han tenido la suficiente diligencia para filtrar información real de la falsa. Por ello, la incorporación de este tipo de pruebas requiere de una adecuada revisión y tratamiento de cara a la actual era de la digitalización y propagación vertiginosa de información de toda clase (González, 2017, p. 145). En razón a ello, se ha atendido a nivel internacional el impacto negativo que puede causar la información digital manipulada proveniente de medios tecnológicos (Simarro, 2020, p. 227).

En el marco legislativo, se ha analizado la posibilidad de que las autoridades pertinentes puedan emprender medidas de investigación en el ciberespacio cuando los marcos jurídicos existentes no sean suficientes, especialmente sí se considera que pruebas como las digitales pueden tener lugar en diversas jurisdicciones, precisamente porque una de sus características es la transnacionalidad. Ello se constituye en una preocupación por la ausencia de un tratamiento diferenciado en los procedimientos penales por ciberdelitos con empleo de pruebas digitales (Consejo de la Unión Europea, 2016).

Si bien los actuales sistemas de justicia han implementado mecanismos para «incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como obtener pruebas electrónicas o digitales de los delitos», como señala el Convenio de Budapest (2001), aún persisten el riesgo y el empleo de redes informáticas y de información electrónica para cometer y ocultar delitos, especialmente con el avance constante y sofisticación de la tecnología a la que tiene acceso la mayoría de la población mundial.

Ahora bien, cabe la pregunta sobre si es necesario poner atención al peligro que podría sufrir el proceso judicial de incorporarse pruebas digitales manipuladas, cuyo origen es reconocido o que han sufrido contaminación durante su recopilación. Es en razón de las graves consecuencias que podría generar una inadecuada actividad probatoria de las pruebas digitales para el debido esclarecimiento de ciberdelitos, que la Unión Europea está preparando una ley de servicios digitales para regular los algoritmos de las grandes plataformas y combatir las campañas de desinformación que pueden desestabilizar la democracia (Consejo de la Unión Europea, s. f.).

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

Así, en el momento de la obtención se analizarán los problemas para determinar el origen, localización y traslado de las pruebas digitales[16], así como la importancia de la cadena de custodia digital para una mejor preservación e integridad de dichas pruebas. Como bien lo refiere un sector de la doctrina, «un acto en apariencia tan inocente como la impresión de una imagen, un correo, o mensajes enviados por WhatsApp, para su ulterior aportación e ingreso al proceso judicial» (Carrasco, 2016, p. 40), puede suponer la omisión de importantes datos de los que puede depender la valoración de la prueba electrónica.

A ello se suma que el peligro de que no se deje constancia de la integridad de los medios en que se almacenaba originalmente la información, y en particular de su preservación a efectos de posteriores comprobaciones e informes (Carrasco, 2016, p. 44). De ahí que, como lo refieren Bielli y Ordóñez (2019, p. 363), «es importante que el juez pueda acceder al documento electrónico en su estado original y con pleno resguardo de todas sus propiedades y no así a un archivo clonado de baja calidad, o una copia impresa del mismo».

Así, por ejemplo, en la fase de admisión, al igual que los medios de prueba tradicionales, debe analizarse los principios de relevancia, la necesidad de aportar información sobre su autenticidad[17] y la posibilidad de recurrir a la prueba pericial forense digital a través de «la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados por medios electrónicos»[18]. Ello brindará información especializada para el mejor análisis, actuación y valoración de este

16 La sola recabación de pruebas digitales puede constituir un problema. Se cuestiona, por ejemplo, la necesidad de solicitar pruebas electrónicas (como correos electrónicos, textos o mensajes en aplicaciones) directamente a un prestador de servicios, lo que constituye un reto procedimental.

17 La autenticidad es un atributo que deben poseer las pruebas que representan un hecho o expresan una voluntad mediante un soporte documental o virtual. Anderson *et al.* (2015) consideran que la autenticidad en los medios de prueba es el elemento más importante de credibilidad de la prueba. En su opinión, «la credibilidad involucra más de una dimensión o atributo, independientemente de qué tipo de prueba se esté considerando [...] los atributos específicos de la credibilidad dependen de qué tipo de prueba estemos considerando» (p. 99).

18 Los dispositivos digitales son una fuente de información fundamental para la investigación de todo tipo de delitos, pero la recopilación y comprensión de pruebas en formato electrónico («pruebas electrónicas» o «pruebas digitales») puede definitivamente resultar difícil.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

tipo de pruebas, especialmente si consideramos que los órganos decisores podrían no estar debidamente formados en el campo de la tecnología[19-20].

En ese sentido, por ejemplo, Galvis y Bustamante (2019) refieren que incluso los metadatos de una prueba electrónica podrían estar sujetos a modificación o alteración, «lo que, a los ojos de alguien sin la experiencia y el conocimiento suficientes, podría generar la creencia de hechos que jamás ocurrieron o que están manipulados y tergiversados» (p. 216)[21-22].

5. Principios y garantías del proceso penal a la luz del nuevo escenario digital

Corresponde ahora profundizar en una perspectiva diferente, pues tanto el proceso penal como los actos que lo conforman, así como sus principios y garantías, requieren revaluarse para determinar si están pensados para delitos cuya ejecución se da no solo en espacios físicos, sino también en entornos o contextos

19 «El análisis forense digital es una rama de la policía científica centrada en la detección, adquisición, tratamiento, análisis y comunicación de datos almacenados por medios electrónicos. Las pruebas electrónicas están presentes en casi todas las actividades delictivas, por lo que el apoyo que proporciona el análisis forense digital es fundamental para todas las investigaciones que llevan a cabo las fuerzas del orden. Tales pruebas pueden extraerse de una amplia gama de fuentes, como, por ejemplo, ordenadores, teléfonos inteligentes, soportes de almacenamiento a distancia, sistemas aéreos no tripulados o aparatos náuticos. El objetivo principal del análisis forense digital es extraer datos contenidos en pruebas electrónicas, transformarlos en información de utilidad operativa y presentar las conclusiones con miras a la persecución penal. En todas las fases del proceso se utilizan avanzadas técnicas forenses, a fin de que las conclusiones resulten admisibles ante un tribunal» (Interpol, s. f.a).

20 «Sin unas capacidades eficaces en materia de análisis forense digital, es probable que los organismos encargados de la aplicación de la ley no lleguen a recopilar pruebas esenciales, o puedan equivocarse en cuanto a su contenido o relevancia o, incluso, las destruyan sin querer» (Interpol, s. f.b)

21 En la normativa comparada, como el Electronic Communications Act del año 2000 y la Electronic Signature Regulation de 2002, la fiabilidad de la prueba informática o electrónica se garantiza con la exigencia del cumplimiento de condiciones especiales con relación al funcionamiento y el uso de las computadoras (Taruffo, 2008, p. 87). Es decir, su calidad también estaría relacionada con el mantenimiento y conservación de los equipos.

22 En este espacio podría discutirse el conocimiento del juez frente a las pericias digitales. Como acota Oteiza (2018), asumir que el juez carece de una formación que le permita ahondar sobre conocimientos especiales imprescindibles para resolver problemas técnicos y científicos plantea un número considerable de cuestiones epistemológicas, «lo cual lleva a especular sobre el nexo que se establece entre quien posee esos conocimientos específicos y quien controla los procesos que llevan a adoptar determinadas conclusiones sobre los hechos» (p. 309).

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

virtuales; y que, sumado a ello, emplean un tipo de prueba especial, la prueba digital, a diferencia de los medios de prueba más tradicionales, como las pruebas testimoniales o las documentales (Caprioli, 2019, pp. 45-46)[23]. Así, por ejemplo, cabe analizar los principios del debido proceso, del derecho de defensa, de la presunción de inocencia y de la prueba, inmediación, contradicción, publicidad e impugnación, para determinar el impacto que ha tenido la nueva criminalidad en su configuración.

El siguiente acápite se enfocará en tres principios específicos: libertad probatoria, inmediación y contradicción.

5.1. Principio de libertad probatoria

El fundamento del derecho a la prueba posee configuración legal: por imperio de este, se confiere a las partes la posibilidad de ingresar todos aquellos medios probatorios relevantes que acrediten su pretensión y que tiendan a garantizar su defensa. Se ha considerado que este derecho forma parte del derecho de defensa, según lo ha establecido el Tribunal Constitucional peruano en el Expediente N.° 010-2002-AI/TC (2003).

El derecho a la prueba posee una vinculación con la búsqueda de la verdad. Por ejemplo, en 1987 la Corte Constitucional italiana, en su Sentenza 146/1987, argumentó que la limitación de la búsqueda de la verdad es contraria a la garantía constitucional del derecho a la defensa. Esta vinculación es expuesta por Ferrer (2016, pp. 51-52), quien expresa que la idea principal del derecho a la prueba es que el ciudadano tenga «derecho a demostrar la verdad de los hechos en los que fundamenta su pretensión». Ello significa, en otros términos, que «todo sujeto procesal tiene derecho a probar si se han producido o no los hechos a los cuales el derecho atribuye sus consecuencias jurídicas».

Ferrer (2016) analiza cuáles serían los elementos definitorios que comprenden el derecho a la prueba y los resume esquemáticamente del siguiente modo:

23 Como lo expone Caprioli (2019): «Quel che è certo è che lo sviluppo tecnologico sta travolgendo l'intera nostra dogmatica della prova, ancora costruita sul modello della prova dichiarativa come ai tempi della Rivoluzione francese. Contraddittorio, oralità, immediatezza cominciano ad assumere un fascino vintage da film storico in costume. Altrettanto certo è che la tecnologia ha ormai assunto le fattezze di un autentico sistema regolativo dei rapporti umani, che affianca il diritto e deve relazionarsi con il diritto esattamente come gli altri sistemi regolativi (l'economia, la società). Il diritto – ivi compreso il diritto delle prove penali – non può sottrarsi al confronto» (pp. 45-46).

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

- Derecho a utilizar todas las pruebas de las que disponen las partes para demostrar la verdad de los hechos que pretenden alegar. Puntualiza que «la única limitación intrínseca a la que está sujeto el derecho a la prueba es la relevancia» (p. 52).
- Derecho a que las pruebas sean practicadas en el proceso.
- Derecho a una valoración racional de las pruebas practicadas.
- Obligación de una debida motivación (pp. 52-58).

El primer contenido del derecho a la prueba —es decir, el derecho a que las partes utilicen todas las pruebas con las que cuentan— es el que está relacionado con la fase de admisión probatoria; en consecuencia, se podrá sostener que este derecho favorece el interés y refuerza el fundamento epistémico de la relevancia (De Paula Ramos, 2013, pp. 290-291), porque permitirá, junto al principio de inclusión, que el ingreso de pruebas relevantes sea una regla de admisión general.

Los principios que regulan el momento de proposición y admisión probatoria son aquellos relacionados con la licitud, pertinencia, idoneidad y utilidad para esclarecer el hecho investigado (Parra, 2007, p. 15). La libertad probatoria permite la adaptación del proceso penal a la evolución tecnológica y social. Ahora, con la irrupción de la cibercriminalidad, hay nuevas fuentes de información: correos electrónicos, mensajes de WhatsApp o Telegram, registros de actividad, *blockchain*, huellas de red, bases de datos en la nube, videos o imágenes generadas digitalmente. El principio de libertad probatoria permitiría su incorporación, aunque no estén previstas expresamente en la ley.

Ahora bien, como antes se ha señalado, la prueba digital es especialmente vulnerable, por lo que la libertad probatoria debe coordinarse con determinadas exigencias de fiabilidad. Por ello, puede establecerse un límite a la autenticidad, por lo que podría admitirse solo lo que pueda acreditarse como auténtico. En lo digital, esto exige: metadatos, *hash* de integridad y validación pericial. Asimismo, se requeriría un límite adicional a la integridad de las pruebas digitales, por lo que cualquier alteración, edición o manipulación invalida la prueba. Por ello, se requiere una cadena de custodia digital que atienda a la preservación de la fiabilidad, el análisis informático forense y la preservación de datos, de ser el caso.

Habría además que repensar el límite de la licitud de las pruebas digitales en tanto que su obtención no podría ampararse en los medios adquiridos a través de hackeos, accesos ilícitos, capturas sin consentimiento en comunicaciones privadas o intrusiones a dispositivos sin orden judicial. Debe estar presente una noción del principio de proporcionalidad, en tanto que el uso de medios digitales

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

de obtención debe respetar la privacidad, los datos personales y los derechos de terceros, especialmente en investigaciones de cibercriminalidad.

La prueba digital permite reconstruir hechos complejos, transnacionales y dinámicos, mientras que la libertad probatoria facilita su recepción y evita que el proceso penal quede obsoleto frente al avance tecnológico. Pero esta libertad no es absoluta: requiere reglas de autenticidad, integridad y fiabilidad sin las cuales la admisión de pruebas digitales pondría en riesgo la verdad procesal.

La libertad probatoria es la puerta de entrada de la prueba digital, el primer contacto con el proceso judicial, pero su ejercicio debe armonizarse con garantías reforzadas, pues no todo lo digital es automáticamente fiable, tal como se pensaría de las pruebas periciales (Gascón, 2010, p. 85). También en el caso de las pruebas digitales, la libertad probatoria exige criterios técnicos y jurídicos estrictos para su validez que conviene trabajar, especialmente en investigaciones de delitos informáticos donde la manipulación es relativamente sencilla.

La doctrina ha sido conteste al considerar que «el juicio es la etapa principal del proceso porque es allí donde se 'resuelve' o 'redefine' de un modo definitivo el proceso» (Binder, 1993, p. 233). Y es que justamente es relevante en este punto porque toman protagonismo dos importantes principios: la inmediación y la contradicción, principios orientadores del sistema procesal penal.

5.2. Principio de inmediación

El principio de inmediación constituye un eje estructural del proceso judicial. Bentham (1971) ya advertía su relevancia, especialmente en relación con la prueba testimonial, al sostener que la exposición oral de los hechos permite aclarar pasajes imprecisos del relato y contrastar directamente las declaraciones con lo consignado en los documentos procesales. A su vez, la intervención directa del juez frente a quienes participan en el proceso le posibilita apreciar elementos significativos del comportamiento, tales como la expresión corporal, la modulación de la voz, las reacciones emocionales y la presencia de indicios de veracidad o de mala fe. Todos estos aspectos han sido trabajados tradicionalmente, aunque ahora han sido vistos de manera crítica. En uno y otro caso, cuando hablamos de pruebas digitales y su inmediación, ya no es posible tratar estos aspectos puesto que las pruebas digitales tienen como característica presente su inmaterialidad.

Como refiere Irrisarri (2021):

> desde la doctrina procesal clásica, Chiovenda (1906) vinculó la inmediatez con una mayor celeridad del proceso, al considerar que el contacto directo

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

> entre las partes favorece una comprensión recíproca que permite exponer con mayor claridad los argumentos ante el tribunal (p. 3).

Esta interacción inmediata, a su vez, facilita una valoración más auténtica y espontánea de las declaraciones. En una línea similar, Carnelutti (1930, p. 173) destacó que la inmediación genera un entendimiento directo entre quien se expresa y quien recibe el mensaje al suprimir distancias y obstáculos que no se limitan al plano material. En efecto, el autor subrayó que dicha proximidad opera no solo en el ámbito físico, sino también en el espiritual, pues los gestos, la forma de hablar y el tono de la voz contribuyen de manera decisiva a la comprensión de la declaración.

En ese entender, la noción clásica del principio de inmediación como medio que posibilita que el juez tenga un contacto directo, personal e ininterrumpido con la prueba, de tal forma que la ausencia de interferencia garantiza que su valoración se base en percepción propia y no en intermediarios, podría igualmente tener algunas consideraciones criticables que analizar. Así, por ejemplo, la doctrina racionalista de la prueba ha sostenido que dicha interpretación podría generar problemas en la valoración, pues se estaría obteniendo inferencias a partir de aspectos enteramente físicos de los sujetos del proceso. «Siendo el juzgador inmóvil es absolutamente necesario trasladar a su presencia los hechos de la realidad, o, mejor, el pedazo de la realidad, pretérita o actual interesante para el proceso» (Serra, 2023, p. 324).

Ahora bien, el principio de inmediación toma especial protagonismo en la actuación de la prueba testimonial, pero no así cuando nos encontramos frente a la práctica de la prueba digital. En ese sentido, habría que replantear cuál es el valor de la inmediación respecto a este medio de prueba. Entonces, si en la prueba testimonial la inmediación permite al juez observar gestos, aspectos físicos y comportamiento del testigo, ¿qué puede observar de manera directa el juez en las pruebas digitales, si muchas de ellas pueden estar contenidas en soportes, pero requieren una interpretación adicional? Incluso, algunas pueden no siempre estar traducidas al lenguaje natural, lo que dificultará sostener que este principio es en alguna medida importante para el desarrollo correcto de la práctica de la prueba; es más, habría que replantearse si es prescindible cuando estamos frente a un proceso por cibercriminalidad que emplee pruebas digitales.

Tradicionalmente, este principio se anclaba en la oralidad, la actuación probatoria en audiencia y la observación directa de los medios personales o documentales, pero podría hablarse de una ruptura en el paradigma tradicional ante la prueba digital. En ese sentido, cuando se trata de los denominados «ciberdelitos» o «delitos informáticos», o en aquellos en los que intervienen entornos

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

virtuales (fraudes electrónicos, *grooming*, suplantación, acceso ilícito, ataques a sistemas), la prueba no surge de un objeto físico perceptible, sino de huellas o registros electrónicos, tales como registros de actividad, metadatos, mensajes instantáneos, contenido de información y datos alojado en la nube, *wallets*, direcciones IP, etc. Estos indicios no son visibles ni comprensibles sensorialmente, requieren herramientas especializadas para ser extraídas, dependen de infraestructura tecnológica (servidores, redes, algoritmos) y pueden alterarse sin dejar rastros evidentes si no hay protocolos adecuados.

Así, la inmediación tal cual ha sido concebida por la doctrina ya no puede ser entendida como percepción directa del contenido digital, sino como control directo del procedimiento técnico que asegura su integridad. La inmediación debe ser concebida como un mecanismo cognoscitivo, como un control procedimental y técnico. De ahí que no se limite a la observación del documento expresado en soporte material, sino que además se debería conocer en juicio cómo se realizó el acto de incautación o el acta de incautación a través de la cadena de custodia digital, así como el proceso de duplicación forense, la verificación de *hash* y la trazabilidad de la cadena de custodia digital. De esta manera, el contacto judicial se orienta a supervisar que la prueba no haya sido contaminada, manipulada ni degradada.

En caso de que se produzca la intervención de la pericia informática, en la audiencia se realizará la exposición del perito informático, con la demostración técnica de cómo se obtuvo la información contenida en redes o en el espacio virtual. De ser el caso, sería necesaria además la explicación visual o demostrativa de metadatos, *timelines* o reconstrucciones de la información obtenida, dado que el órgano jurisdiccional debería cumplir un rol activo que involucra no solo la escucha, sino también las consultas y preguntas necesarias durante la presentación (Serra, 2023, p. 2352)[24].

Si se interpretara la inmediación, podría sostenerse que el juez «ve» la prueba no en su estado original, sino a través de su proceso validado. Asimismo, corresponde que la inmediación involucre que el juez evalúe directamente la credibilidad técnica del análisis, verifique la consistencia de protocolos para el uso

24 Al hablar de prueba pericial, Serra Domínguez (2023) refiere que hay una dificultad de control crítico del juez sobre los resultados de la pericia. Así, sostiene que «si el juez tiene un conocimiento inmediato —reconocimiento judicial— o mediato —documento, confesión, testigos— de los hechos apreciados con arreglo a los conocimientos técnicos proporcionados por el perito, podrá discrepar de sus conclusiones; pero si solo conoce los hechos y la máxima de experiencia a través del dictamen pericial, le resultará imposible efectuar una revisión crítica de las conclusiones del perito» (p. 2352).

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

de determinada prueba digital en el cibercrimen, o identifique las limitaciones o márgenes de error. Es decir, la inmediación deja de centrarse en el objeto digital y se desplaza hacia el acto técnico que lo produce. Recordemos que, como lo refiere Serra (2023), en las pruebas el proceso intelectual es tan rápido que la mente no lo advierte y lo verifica mecánicamente, debiendo solo desarrollarse de este modo si atiende al hecho probatorio (p. 2576).

Se puede sostener inicialmente que la prueba digital reconfigura la inmediación; en ese sentido, precisamente por tratarse de hechos electrónicos, los jueces no tienen contacto directo con el dato original, sino con el proceso técnico que garantiza su autenticidad. Esta reinterpretación es indispensable en delitos de cibercriminalidad donde la evidencia reside en entornos volátiles, distribuidos y, sin duda, técnicamente complejos.

5.3. Principio de contradicción

El principio de contradicción se constituye en uno de los pilares del proceso judicial que tiene lugar en la fase oral del juicio en tanto se ejerce a través de la oposición de argumentos y razones entre las partes sobre las cuestiones introducidas que constituyen el objeto de prueba, facilitando el control de la actividad de la parte contraria mediante la exposición de argumentos, la discusión de pruebas y el debate, entre otros recursos (Neyra, 2015, p. 516). En términos de Ferrajoli (1998), el principio de contradicción es el más «importante instrumento de impulso y control del método de prueba en un sistema acusatorio, consistente en la contraposición entre hipótesis de acusación y de defensa y las pruebas y contrapruebas correspondientes» (p. 613). Para añadir estas posturas, Igartua (2009) considera que el principio de contradicción es una garantía epistemológica para la determinación de la verdad de los enunciados fácticos a probar (p. 162).

El momento del contradictorio permite una confrontación directa de las partes respecto a las pruebas presentadas (digitales, testimoniales y periciales, entre otras) en la que se hace ejercicio del derecho de defensa a través de la contradicción, de ahí que se haya asumido al proceso como un escenario de confrontación entre las partes. Ahora bien, que la confrontación sea entre las partes no limita el rol del juez al de un órgano pasivo y observador del proceso; por el contrario, si se pretende obtener la mayor información posible para reconocer un medio de prueba fiable[25] y, además, realizar adecuadamente la valoración

25 Como cualquier hecho derivado de un medio de prueba, tendrá mayor o menor solidez, dependiendo de la calidad epistemológica de los medios y los grados de inferencia para fijarlos.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

—especialmente cuando se está frente a un contexto donde las pruebas no son las tradicionales, sino que emplean conocimientos técnicos o tecnológicos (prueba pericial y prueba digital) que son ajenos al saber jurídico—, la participación del órgano jurisdiccional es necesaria. Como bien lo expone Serrá Domínguez (2023), «uno de los problemas prácticos que debe resolver la ciencia procesal es el relativo a la limitación de conocimientos del juez, unida a la cada vez más creciente complejidad de la vida moderna» (p. 2327).

Así, en el entendido que nos encontramos frente a un proceso penal que requiere de conocer los hechos de índole digital o que emplea las herramientas de la tecnología y la comunicación, el contradictorio no solo podría limitarse únicamente a un conflicto o combate dialéctico entre las partes del proceso (Taruffo, 2013, p. 242), sino que requiere que se respeten las garantías mínimas que debe ofrecer toda actividad probatoria, más aún a la luz de un nuevo contexto de expansión de la cibercriminalidad. En esa línea, no se trata solo de que la contradicción sea concebida como una lucha entre partes donde estas pueden utilizar indistintamente cualquier método (legítimo o no) para ingresar medios de prueba alegando su desconocimiento o, incluso, para ocultar pruebas o interponer obstáculos procesales; sino que ello implicaría que el empleo de la contradicción —desde esta perspectiva— estaría causando un desmedro al desarrollo de un proceso justo y, por el contrario, alentaría la mala fe procesal.

Desde una concepción epistémica del proceso como la asumida por el profesor italiano Taruffo (2005),

> el contradictorio ha de ser entendido como un método de formación de la prueba que aspira a asegurar, mediante la confrontación de las posiciones, informaciones y argumentaciones diversas, proporcionadas por las partes, la plenitud y fiabilidad del procedimiento probatorio y de los criterios de decisión sobre los hechos (p. 428).

Entonces, la contradicción debe ser entendida como un método de adquisición de conocimiento e información requerida para determinar o esclarecer los hechos objeto de prueba, pero además como instrumento que garantiza la igualdad de armas en el desarrollo del proceso judicial; esto es, como una herramienta cognoscitiva (Vázquez, 2015, p. 187).

Las distintas pruebas o elementos de juicio deben cumplir una función corroboradora de los aspectos que integran la hipótesis fáctica que se pretenda probar (Ferrer, 2007, p. 86). El modo de implementar jurídicamente mecanismos que faciliten dicha corroboración es el denominado «principio de contradicción». Así, este principio permite los siguientes controles probatorios:

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

1. Un control sobre la correcta aplicación de las reglas epistemológicas y jurídicas sobre la admisión probatoria.
2. La práctica de la prueba de forma contradictoria.
3. La posibilidad de proponer pruebas contrarias a las ofrecidas por la otra parte procesal, de modo que permita vencer y/o corroborar una hipótesis fáctica distinta e incompatible.
4. La posibilidad de proponer pruebas de segundo orden (prueba sobre prueba) que impugnen la fiabilidad de pruebas ofrecidas por la otra parte (Ferrer, 2007, pp. 87-88).

En ese sentido, el principio de contradicción asegura que las partes del proceso puedan conocer, discutir, impugnar y confrontar los elementos probatorios. Este principio es central para la igualdad de armas y permite a la defensa participar activa y eficazmente en la actividad probatoria. Ahora bien, en el contexto del presente trabajo, cuando estamos frente a un proceso penal donde la prueba presente para la investigación de un ciberdelito es la prueba digital, pueden presentarse algunos inconvenientes para el pleno ejercicio del principio de contradicción. En escenarios de cibercriminalidad, la contradicción enfrenta desafíos particulares:

- La prueba digital puede requerir conocimientos altamente técnicos y muchas veces tanto el órgano judicial como las partes procesales, incluida la defensa, carecen de conocimientos o recursos para comprenderla, lo que dificulta el nivel del debate y del contradictorio. Esta dificultad podría disminuir con la asistencia de una pericia, pero no todos los casos ameritan que se presente una «prueba sobre prueba»; esto es, que no todas las pruebas digitales deberían requerir que se emita un informe pericial al respecto.
- Otro de los problemas que puede afrontarse en el contradictorio de las pruebas digitales es que, además de depender en ocasiones del conocimiento especializado, no todas las pruebas digitales tendrán acceso abierto o público, pues muchas de estas poseen naturaleza privada, son inaccesibles o de código cerrado, y por más que se conozca de su existencia, no así su contenido.
- Las pruebas digitales pueden encontrarse en servidores extranjeros sujetas a cooperación internacional, lo que dificulta su revisión; o, en el peor de los casos, son completamente inaccesibles. Ello se debe a que, en el marco de la cibercriminalidad, las pruebas digitales primordialmente tienen como característica la transnacionalidad. Así, muchos de

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

los delitos que atacan directamente datos e información relevante de empresas o entidades estatales e internacionales pueden tener como lugar de comisión un determinado país, pero sus efectos pueden ser generados en otros.

- Ahora bien, en el caso de que las pruebas digitales sí se hayan presentado al proceso e ingresen al contradictorio, no siempre tendrán una forma tangible de ser presentadas. También en ese caso, la simple visualización del contenido no garantiza su autenticidad, integridad o el contexto de las pruebas digitales que son debatidas en el contradictorio.

En definitiva, hay probabilidad de que esta asimetría técnica y de conocimientos y saberes digitales genere una desigualdad real que amenace el ejercicio pleno de la contradicción. En ese sentido, cabe la posibilidad de requerir un sistema de contradicción con ciertos aspectos a tener en consideración cuando estamos frente a pruebas digitales en un contexto de cibercriminalidad[26].

De ahí que resultaría indispensable un acceso que sea lo más íntegro posible a las pruebas digitales porque su complejidad sobrepasa la entrega de capturas de pantalla o extractos de conversaciones, y, además, los cibercriminales pueden dejar huellas o rastros en la misma red que conforma el ciberespacio. Su acceso, por tanto, podría ser más complicado porque no estamos siempre frente a datos que pueden presentarse mediante pruebas documentales y en soportes físicos; por ejemplo, los *hash* de verificación, los *logs* originales, los metadatos completos, siempre en el supuesto que todos estos tenga relevancia y puedan así discutirse en el juicio. Sin ello, la contradicción sería meramente una formalidad.

Sin necesidad de la prueba pericial informática, la prueba digital en el contradictorio ameritaría que se pueda conocer el *software* y la metodología de obtención; en ese sentido, al ser un medio de prueba de índole especializada, deberían conocerse los mecanismos utilizados para la extracción, así como su versión, su margen de error, si es *software* abierto o cerrado, y si permite replicar los resultados.

Además, en caso de que se presente la pericia informática, las partes —como la defensa— podrían presentar una pericia de parte independiente para que pueda

26 Ello porque bien podrían presentarse pruebas digitales en marcos delictivos diversos a un escenario de cibercriminalidad. Por ejemplo, cuando hablamos de la presentación de conversaciones por correo electrónico para procesos de despidos laborales, no estamos propiamente ante un hecho delictivo perteneciente al marco de la cibercriminalidad y sí, en cambio, al de delitos tradicionales que hacen uso de pruebas digitales.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

ser contrapericia a la de oficio. Ahora bien, el ejercicio de la contradicción no se logra solamente interrogando al perito, sea de oficio o de parte, sino que debe garantizarse la posibilidad de designar un perito de parte, replicar la extracción, reproducir la verificación del *hash* y confrontar metodologías.

Asimismo, debe tenerse presente que, en el escenario o contexto digital, una vez producidos los delitos informáticos, el contenido aislado puede ser engañoso. Esto significa que la contradicción exige evaluar un contexto temporal (*timelines*), la correlación de eventos, el origen y el destino de mensajes, comunicaciones y fechas, además de las posibles manipulaciones que pudieron haber atravesado el proceso y el resultado. No se trata solo y exclusivamente de lo que la prueba digital muestra, sino que esta información puede estar vinculada con datos adicionales de conocimiento necesario para su completa comprensión en juicio.

La contradicción en prueba digital implica acceso técnico equitativo y, de ser el caso, y siempre que lo permita así el medio de prueba, la replicabilidad del análisis. Sin transparencia de metodología ni conocimiento de las herramientas de obtención, sin copia forense y sin posibilidad real de contrapericia, la contradicción no cumpliría un rol de adquisición de conocimiento y de contenido, especialmente en procesos por cibercriminalidad donde la complejidad técnica es alta y la manipulación es posible.

6. Conclusiones

La expansión de la cibercriminalidad y la creciente incorporación de tecnologías en la vida social, económica y comunicacional han transformado profundamente el modo en que se obtienen, introducen y valoran las pruebas en el proceso penal. Este escenario exige replantear categorías y principios construidos históricamente para un modelo de criminalidad tradicional desarrollada en espacios físicos, con medios de prueba tangibles y fácilmente perceptibles. La irrupción de la prueba digital —caracterizada por su fragilidad, volatilidad, posibilidad de manipulación y naturaleza transnacional— revela los límites del sistema probatorio clásico y confirma la necesidad de una valoración racional y epistémica que permita afrontar adecuadamente los desafíos que plantea el entorno digital.

En primer lugar, la investigación demuestra que los sistemas judiciales requieren de un tratamiento procesal y probatorio diferenciado para las pruebas digitales, atendiendo a su origen tecnológico, al carácter dinámico de los datos en entornos informáticos y a la facilidad con la que pueden ser alterados o destruidos. La ausencia de mecanismos específicos para su obtención, conservación y

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

verificación compromete la fiabilidad de la información que ingresa en el proceso y, con ello, la capacidad del Estado para sancionar efectivamente los ciberdelitos.

En segundo término, se constata que los principios de libertad probatoria, inmediación y contradicción necesitan ser reinterpretados a la luz del nuevo ecosistema digital. La libertad probatoria permite la incorporación de nuevas fuentes de información, pero únicamente bajo estrictas garantías de autenticidad e integridad. La inmediación, tradicionalmente vinculada a la percepción directa del juez, debe reorientarse hacia el control del proceso técnico de producción, extracción y validación de la prueba digital. A su vez, la contradicción enfrenta importantes obstáculos derivados de la complejidad tecnológica, la disparidad de conocimientos entre las partes y la posible inaccesibilidad a los datos originales, factores que pueden generar una desigualdad real en el debate procesal.

Asimismo, la investigación evidencia que una actividad probatoria racional de la prueba digital exige integrar conocimientos interdisciplinarios, en particular aquellos provistos por las ciencias informáticas y la informática forense. La pericia digital se convierte en un instrumento esencial para garantizar que los datos presentados sean auténticos, íntegros y verificables, así como para dotar al órgano jurisdiccional de herramientas cognitivas suficientes para su adecuada valoración.

Finalmente, se concluye que la apreciación racional de la prueba digital constituye una necesidad impostergable para los sistemas de justicia contemporáneos. Frente al crecimiento de los ciberdelitos y al uso sofisticado de tecnologías para ocultar o manipular información, la respuesta estatal debe orientarse hacia la creación de criterios técnicos y jurídicos claros que aseguren la preservación, admisión y valoración fiable de la evidencia digital. Solo así se garantizará el esclarecimiento de los hechos, la protección de derechos fundamentales y la efectividad del proceso penal en un entorno en constante transformación.

En suma, la presente investigación pone de manifiesto que la cibercriminalidad no solo desafía al derecho penal sustantivo, sino también a la teoría de la prueba y a los principios estructurales del proceso. Adaptarse a esta nueva realidad demanda una reconstrucción racional del sistema probatorio, capaz de integrar el conocimiento tecnológico sin renunciar a los valores que sustentan un proceso penal justo: verdad, defensa, transparencia, fiabilidad y control epistémico de las decisiones judiciales.

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007

Bibliografía

Abel Lluch, X. (2011).
Prueba electrónica. En Xavier Abel Lluch y Joan Picó i Junoy (dirs.), *La prueba electrónica* (pp. 15-230). Barcelona: Bosch Editor.

Anderson, T., Schum, D., & Twining, W. (2015).
Análisis de la prueba (F. Carbonell y C. Agüero, trads.). Madrid: Marcial Pons.

Andrés Ibáñez, P. (2003).
Sobre el valor de la inmediación. (Una aproximación crítica). *Jueces para la democracia*, (46), 57-66. https://dialnet.unirioja.es/servlet/articulo?codigo=409555

Armenta Deu, T. (2018).
Los medios tecnológicos son fuente esencial de diversas investigaciones. *Revista de Internet, Derecho y Política*, (27), 67-78. https://www.raco.cat/index.php/IDP/article/view/n27-armenta

Arbós i Llobet, R., Fons Rodríguez, C., Izquierdo Blanco, P., Queral Carbonell, A., Del Valle García, M., & Pérez Daudí, V. (2011).
La prueba electrónica (Xavier Abel Lluch y Joan Picó i Junoy, dirs.; Núria Ginés Castellet, coord.). Barcelona: J. M. Bosch Editor.

Bielli, M., & Ordóñez, C. (2019).
El juez y la prueba electrónica. Buenos Aires: Colegio de Abogados de Morón.

Binder, A. (1993).
Introducción al Derecho Procesal Penal (2.ª ed.). Buenos Aires: Ad Hoc.

Carnelutti, F. (1930).
Derecho y proceso (S. Santis Melendo, trad.). Buenos Aires: Ediciones Jurídicas Europa-América.

Carrasco M., S. (2016).
La alegalidad o limbo legal de la prueba electrónica. En Ricardo Oliva León y Barceló Valero (coords.), *La prueba electrónica. Validez y eficacia procesal* (pp. 40-49). Juristas con Futuro. https://dialnet.unirioja.es/servlet/libro?codigo=658404

Caprioli, F. (2020).
Tecnologia e prova penale: nuovi diritti e nuove garanzie. En *Dimensione tecnologica e prova penale* (pp. 45-54). Turín: Giappichelli.

Comisión Europea. (2020).
Estrategia de ciberseguridad de la UE. https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-strategy

Consejo de la Unión Europea. (s. f.).
Ley de Servicios Digitales. https://www.consilium.europa.eu/es/infographics/digital-services-act/

Consejo de la Unión Europea. (2016).
Lucha contra las actividades delictivas en el ciberespacio: el Consejo acuerda medidas prácticas y los próximos pasos. https://www.consilium.europa.eu/es/press/press-releases/2016/06/09/criminal-activities-cyberspace/

Consejo de la Unión Europea. (2021).
Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy [comunicado de prensa]. https://www.consilium.europa.eu/es/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

Consejo de la Unión Europea. (2024).
Ciberseguridad: estrategia y políticas clave de la UE. https://www.consilium.europa.eu/es/policies/cybersecurity/

De Paula Ramos, V. (2013).
Derecho Fundamental a la prueba. *Gaceta Consstitucional*, (65), 286-299.

Elías Puelles, R. (2025).
Delitos contra la seguridad informática. Acceso ilícito, atentados contra la integridad y disponibilidad de datos y sistemas informáticos, interceptación ilícita de datos informáticos, abuso de dispositivos. Lima: Instituto Pacífico y Actualidad Penal.

Fernández, M. (2005).
Prueba y presunción de inocencia. Madrid: Iustel Publicaciones.

Ferrajoli, L. (1998).
Derecho y razón. Teoría del garantismo penal (Perfecto Andrés Ibañez y otros, trads.). Madrid: Editorial Trotta.

Ferrer Beltrán, J. (2007).
La valoración racional de la prueba. Madrid: Marcial Pons.

Ferrer Beltrán, J. (2016).
Motivación y racionalidad de la prueba. Lima: Grijley.

Galvis, Á., & Bustamante, M. (2019).
La no equivalencia funcional entre la prueba electrónica y la prueba documental: Una lectura desde la regulación procesal colombiana. *Revista Ius et Praxis*, *25*(2), 189-222. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122019000200189

Gascón Abellán, M. (2010).
Prueba científica. Mitos y paradigmas. *Anales de la Cátedra Francisco Suárez*, (44), 81-103.

González Lage, J. (2017).
La prueba pericial en la práctica judicial penal: las redes sociales en el proceso penal. En Picó i Junoy (dir.), *Peritaje y prueba pericial* (pp. 563-569). Barcelona: Bosh Procesal.

Igartua, J. (2009).
El razonamiento en las resoluciones judiciales. Lima: Palestra.

Interpol. (s. f.a).
Análisis forense digital. https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital

Interpol. (s. f.b).
Proyecto Leader. https://www.interpol.int/es/Como-trabajamos/Innovacion/Projects/Proyecto-Leader

Irisarri, S. M. (2021).
La función epistemológica del principio de inmediación en la prueba testimonial: ¿Garantía procesal? https://dugi-doc.udg.edu/handle/10256/19425.

Miró Llinares, F. (2012).
El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons Ediciones Jurídicas y Sociales.

Naciones Unidas. (s. f.).
ONU llama a superar brechas en el uso de las TIC. https://www.un.org/es/desa/wsis10

Naciones Unidas. (2015).
ONU llama a superar brechas en el uso de las TIC. Departamento de Asuntos Económicos y Sociales. https://www.un.org/es/desa/wsis10

Naciones Unidas. (2021).
Los avances tecnológicos están convirtiendo simples delitos en amenazas mundiales. https://news.un.org/es/story/2021/06/1493862

Neyra Flores, J. A. (2015).
Tratado de Derecho Procesal Penal (t. II). Lima: Idemsa.

Oficina de las Naciones Unidas contra la Droga y el Delito. (s. f.).
Pruebas digitales. https://syntheticdrugs.unodc.org/syntheticdrugs/es/cybercrime/detectandrespond/investigation/digitalevidence.html

Ortiz Pradillo, J. (2013).
La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación. Fundación Alternativas. https://eprints.ucm.es/64640/

Oteiza, E. (2017).
Prueba digital y acceso a la justicia: imparcialidad e igualdad. En Joan Picó i Junoy (dir.), *Peritaje y prueba pericial* (pp. 303-317). Barcelona: Bosch Editor.

Parra, J. (2007).
Manual de derecho probatorio (15.ª ed.). Bogotá: Librería Ediciones del Profesional LTDA.

Requejo-Passoni, W. (2024).
El dilema de las copias de seguridad en el delito de sabotaje contra datos informáticos en el derecho penal español. *IDP: Revista de Internet, Derecho y Política*, (41), 1-12. https://doi.org/10.7238/idp.voi41.420591

Sansurjo Ríos, E. I. (2020).
Proceso penal y volatilidad/mutabilidad de las fuentes de las pruebas electrónicas: sobre la conveniencia y el modo de asegurarlas eficazmente. En Eva Isabel Sansurjo Ríos y Piedad Gónzalez Granda (dirs.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónica* (pp. 195-224). https://dialnet.unirioja.es/servlet/articulo?codigo=7575108

Serra Domínguez, M. (2023).
Obra procesal (t. V-VII, prueba [2.ª parte], pp. 2323-3014). Barcelona: Fundación Privada Manuel Serrá Domínguez.

Simarro Pedreira, M. (2020).
La cadena de custodia en la prueba digital: España vs. EE.UU. En Eva Isabel Sansurjo Ríos y Piedad Gónzalez Granda (dirs.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónica* (pp. 225-237). https://dialnet.unirioja.es/servlet/articulo?codigo=7575107

Taruffo, M. (2008).
La prueba de los hechos (4.ª ed.). Madrid: Editorial Trotta.

Taruffo, M. (2013).
La verdad en el proceso. *Derecho & Sociedad*, (40), pp. 239-248. https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/12804

Vázquez Rojas, C. (2015).
De la prueba científica a la prueba pericial. Madrid: Marcial Pons.

World Economic Forum (WEF). (2014).
Outlook on the Global Agenda 2014. https://www3.weforum.org/docs/WEF_GAC_GlobalAgendaOutlook_2014.pdf

Jurisprudencia, normas y otros documentos legales

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Hacer frente a la desinformación en línea: un enfoque europeo (COM(2018) 236 final) (Comisión Europea, 2018)). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&rid=10

Convenio de Budapest [Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia] (Consejo Europeo, 23 de noviembre de 2001). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Expediente N.° 010-2002-AI/TC (Tribunal Constitucional [Perú], 3 de enero de 2003). https://www.tc.gob.pe/jurisprudencia/2003/00010-2002-AI.html

Recurso de Nulidad N.° 222-2019/Lima (Sala Penal Permanente de la Corte Suprema de Justicia de la República [Perú], 2019). https://img.lpderecho.pe/wp-content/uploads/2020/07/RN-222-2019-Lima-LP.pdf

Reglamento (UE) 2019/881, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Parlamento Europeo y Consejo de la Unión Europea, 17 de abril de 2019). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32019R0881

Sentenza 146/1987 (Corte Costituzionale [Italia], 1987). https://giurcost.org/decisioni/1987/0146s-87.html?utm_source=chatgpt.com

Revista de la Maestría en Derecho Procesal, Vol. 11(1), 2026 (ISSN 2072-7976), pp. 285-316
https://doi.org/10.18800/rmdpro.202601.007