



FACULTAD DE DERECHO

# **LA PRUEBA DIGITAL Y EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS**

Helena Tamarit Sánchez

4ºE1

Área de Derecho Procesal

Madrid

Marzo de 2026

## ÍNDICE

|                                                                                                                                              |           |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN</b>                                                                                                                       | <b>4</b>  |
| 1.1 Contextualización y objetivos del trabajo                                                                                                | 4         |
| 1.2 Estructura y metodología                                                                                                                 | 5         |
| <b>CAPÍTULO I. CONCEPTO, EVOLUCIÓN Y CLASIFICACIÓN DE LOS MEDIOS DE PRUEBA</b>                                                               | <b>7</b>  |
| 1. CONCEPTO Y EVOLUCIÓN DE LOS MEDIOS DE PRUEBA                                                                                              | 7         |
| 1.1 Concepto de los medios de prueba y función en el proceso                                                                                 | 7         |
| 1.2 Evolución de la prueba digital como medio de prueba                                                                                      | 7         |
| 2. CLASIFICACIÓN DE LOS MEDIOS DE PRUEBA EN LA LEY DE ENJUICIAMIENTO CIVIL Y CRIMINAL                                                        | 9         |
| 2.1 Medios de prueba en la Ley de Enjuiciamiento Civil                                                                                       | 9         |
| 2.2 Medios de prueba en la Ley de Enjuiciamiento Criminal                                                                                    | 11        |
| 3. PRINCIPIOS GENERALES Y FINALIDAD DE LA PRUEBA                                                                                             | 12        |
| <b>CAPÍTULO II. LA PRUEBA ELECTRÓNICA Y SU ENCAJE EN EL ORDENAMIENTO PROCESAL, NATURALEZA DE LOS DOCUMENTOS ELECTRÓNICOS Y FIRMA DIGITAL</b> | <b>14</b> |
| 1. LA PRUEBA ELECTRÓNICA Y SU ENCAJE EN EL ORDENAMIENTO PROCESAL                                                                             | 14        |
| <b>CAPÍTULO III. OBJETO DE LA PRUEBA, DIFICULTADES EN EL ACCESO A LA MISMA, VALORACIÓN JUDICIAL Y CADENA DE CUSTODIA</b>                     | <b>20</b> |
| 1. OBJETO DE LA PRUEBA Y DIFICULTADES E ILICITUD EN EL ACCESO A LA MISMA                                                                     | 20        |
| 2. VALORACIÓN JUDICIAL, CARGA DE LA PRUEBA Y GARANTÍAS DE AUTENTICIDAD                                                                       | 23        |
| <b>CAPÍTULO IV. LAS REDES SOCIALES COMO FUENTES DE PRUEBA</b>                                                                                | <b>28</b> |
| 1. LAS REDES SOCIALES COMO FUENTE DE PRUEBA ELECTRÓNICA EN EL PROCESO JUDICIAL                                                               | 28        |
| 1.1 Requisitos jurisprudenciales para la validez de la prueba tecnológica procedente de redes sociales                                       | 28        |
| 1.1.1 Autenticidad del contenido                                                                                                             | 29        |
| 1.1.2 Identificación del titular de la cuenta                                                                                                | 29        |
| 1.1.3 Integridad y preservación de la evidencia                                                                                              | 30        |
| 1.1.4 Posibilidad de contradicción/impugnación                                                                                               | 30        |
| 1.1.5 Confirmación de la veracidad de la prueba tecnológica a través de la pericial informática                                              | 31        |
| 1.1.6 Respeto a los derechos fundamentales                                                                                                   | 31        |
| 2. VALIDEZ Y EFICACIA PROBATORIA DE LAS PRUEBAS DIGITALES PROCEDENTES DE “WHATSAPP”                                                          | 31        |

|                                                                                   |           |
|-----------------------------------------------------------------------------------|-----------|
| 3.EL CORREO ELECTRÓNICO COMO MEDIO DE PRUEBA EN EL PROCESO CIVIL .....            | 35        |
| 4. LA POSIBLE VULNERACIÓN DE DERECHOS FUNDAMENTALES Y LA REGLA DE EXCLUSIÓN. .... | 37        |
| 5.PROTECCIÓN DE DATOS Y VALORACIÓN PROCESAL .....                                 | 39        |
| <b>CAPÍTULO V. IMPUGNACIÓN DEL DOCUMENTO ELECTRÓNICO Y PRUEBA PERICIAL .....</b>  | <b>41</b> |
| 1.CONCEPTO DE IMPUGNACIÓN DE LA PRUEBA EN EL PROCESO CIVIL .....                  | 41        |
| 2. OBJETO Y FINALIDAD. REQUISITOS DEL INFORME .....                               | 43        |
| <b>CONCLUSIONES .....</b>                                                         | <b>47</b> |
| <b>BIBLIOGRAFÍA .....</b>                                                         | <b>50</b> |

## **1. INTRODUCCIÓN**

### **1.1 Contextualización y objetivos del trabajo**

El presente trabajo de Fin de Grado se centra en el régimen jurídico-procesal de la prueba digital, que se ha constituido en el medio probatorio de mayor crecimiento y relevancia tanto en el proceso civil como en el penal. Abarca tanto la prueba electrónica - entendida como el medio de prueba que se aporta en un procedimiento judicial - como el documento electrónico concebido como el soporte digital que incorpora hechos jurídicamente relevantes, ambos dotados con plena eficacia jurídica y procesal si cumplen los requisitos técnicos y procesales que se expondrán.

Se pretende abordar los problemas comunes que la prueba digital plantea en el proceso civil y en el penal, así como las diferencias existentes, destacando en el orden penal las garantías constitucionales como la exigencia de garantizar la cadena de custodia, o la intervención de los dispositivos respetando los derechos fundamentales o en el orden civil, sobre el modo de aportación de la prueba por la parte, la impugnación de la documental electrónica o la valoración judicial de documentos privados electrónicos.

Los medios de pruebas representan una de las partes más importantes del procedimiento judicial ya que se configuran como el instrumento por el que las partes demuestran sus alegaciones para que el juzgador resuelva tras la correspondiente valoración. La elección de este tema responde a la necesidad de comprender las nuevas tecnologías y su integración en el proceso judicial. Pretendo alejarme de los enfoques tradicionales y con ello adoptar una perspectiva innovadora. Asimismo, una de las pretensiones de este trabajo es la proyección clara hacia el futuro del Derecho, intentando analizar y comprender el proceso de adaptación del legislador al nuevo marco normativo derivado de la digitalización.

El estudio de la prueba digital plantea la necesidad de actualización de los medios de prueba a los cambios tecnológicos actuales, así como de garantizar su correcta admisión, práctica y valoración con el fin de asegurar un proceso judicial con todas las garantías y evitar resoluciones insuficientemente motivadas o fundamentadas en pruebas que se puedan catalogar de fraudulentas por no reunir las condiciones tecnológicas que garanticen su integridad.

Partiendo de lo anterior, el objeto del trabajo parte del análisis de la prueba digital en el proceso civil, atendiendo a sus principios rectores y a su regulación legal, junto a su fundamento constitucional y a la interpretación jurisprudencial que han realizado los tribunales hasta el momento. A tal efecto, examinaremos los principales medios de prueba digitales, la carga de los elementos probatorios, los criterios de valoración y requisitos necesarios para su admisibilidad en el proceso, con el fin de valorar si la actual regulación garantiza efectivamente el derecho a la tutela judicial efectiva reconocido en el artículo 24 CE.

Para la elaboración se ha procedido a la investigación de las respectivas leyes reguladoras de las particularidades de la prueba digital, como la Ley de Enjuiciamiento Civil (LEC), Ley de Enjuiciamiento Criminal (LECrim), normativa específica sobre digitalización y administración de justicia digital. Asimismo, he intentado incorporar las posturas de la doctrina científica más relevante sobre esta materia.

Respecto a la jurisprudencia, esencialmente del Tribunal Supremo, se procede a establecer la forma en que la prueba debe ser obtenida, valorada e incorporada al procedimiento judicial junto con los eventuales límites y las inevitables garantías, necesarias para salvaguardar derechos esenciales en el proceso.

## **1.2 Estructura y metodología**

El presente trabajo se ha desarrollado en torno a una metodología jurídico-dogmática, apoyada en el análisis normativo de la legislación procesal civil y penal, realizando un análisis crítico de la doctrina científica, de manera más profunda, la jurisprudencia del Tribunal Supremo y de las Audiencias Provinciales, como interpretativa de las normas y lagunas legales.

Respecto a la estructura, el trabajo se divide en cinco capítulos. El **Capítulo I** sienta las bases conceptuales necesarias, evolución y clasificación de los medios de prueba y los principios generales en materia de actividad probatoria que resultan aplicables al entorno digital.

Posteriormente, el **Capítulo II** se centra en el análisis del encaje de la prueba electrónica en nuestro ordenamiento, su naturaleza jurídica y el papel que desempeña la firma digital.

El **Capítulo III** valora las dificultades que plantea la práctica de la prueba digital, desde el acceso lícito, las consecuencias de la obtención vulnerando derechos fundamentales, criterios de valoración judicial y la trascendencia de la cadena de custodia.

A continuación, el **Capítulo IV** estudia las fuentes de prueba digital más relevantes en la práctica forense: redes sociales, mensajería instantánea y el correo electrónico. Se presta atención a los requisitos jurisprudenciales.

Finalmente, el **Capítulo V** analiza el régimen de impugnación de los documentos electrónicos y los requisitos, objeto y finalidad de la prueba pericial informática, cuando la prueba digital es cuestionada.

Terminaremos con un apartado de **Conclusiones** en el que intentaremos identificar las carencias normativas y se formulan propuestas de *lege ferenda* dirigidas a dotar de mayor seguridad jurídica al tratamiento procesal de la prueba digital.

## **CAPÍTULO I. CONCEPTO, EVOLUCIÓN Y CLASIFICACIÓN DE LOS MEDIOS DE PRUEBA**

### **1. CONCEPTO Y EVOLUCIÓN DE LOS MEDIOS DE PRUEBA**

#### **1.1 Concepto de los medios de prueba y función en el proceso**

Los medios de prueba constituyen una parte de gran relevancia en el procedimiento jurisdiccional en tanto que, a través de ellas, las partes harán valer su posición frente al juez para lograr su convicción<sup>1</sup>. Desde un punto de vista conceptual, la prueba se define como la actividad procesal llevada a cabo para lograr el posicionamiento del Tribunal respecto de la certeza o falsedad de los hechos alegados por las partes, con el objetivo de garantizar un proceso equitativo y justo.

Resulta relevante aclarar la distinción entre medios de prueba y fuentes de prueba. Los medios de prueba se configuran como las actividades procesales necesarias para incorporar la fuente al proceso y las fuentes de prueba son los propios archivos o dispositivos digitales<sup>2</sup>.

La función de los medios de prueba no es otra que la construcción de una actividad probatoria que se practique conforme a los principios generales de contradicción (permitiendo a las partes conocer, debatir y confrontar las pruebas y argumentos presentados por la contraparte), igualdad de armas (facultando a las partes contar con acceso a las mismas facultades para alegar, presentar pruebas, controvertir las de la contraparte e impugnar resoluciones) e inmediación (estando el Juzgador presente en todas las audiencias para percibir, escuchar y observar para valorar la veracidad de las actuaciones), siendo un elemento imprescindible para la motivación de las resoluciones judiciales<sup>3</sup>.

#### **1.2 Evolución de la prueba digital como medio de prueba**

Desde nuestra perspectiva, la evolución de los medios de prueba ha venido condicionada por el proceso de digitalización de las relaciones sociales, económicas y comunicativas que ha

---

<sup>1</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil. Parte General” (14.<sup>a</sup> ed.), *Tirant lo Blanch*, Valencia, 2025, pp. 224-226.

<sup>2</sup> Consejo General del Poder Judicial, “La prueba en el proceso civil, la prueba ilícita y la prueba generada en el seno de las nuevas tecnologías: conclusiones”, *Cuadernos Digitales de Formación*, n.º 24, Madrid, 2018, pp. 4-7,

<sup>3</sup> Ibáñez Rodríguez, A., “El derecho a la prueba como garantía esencial del proceso”, *Hay Derecho*, entrada de 9 de junio de 2025 (disponible en <https://www.hayderecho.com/2025/06/09/el-derecho-a-la-prueba-como-garantia-esencial-del-proceso/>; última consulta 15/03/2026).

provocado un proceso de digitalización de la Administración de Justicia, mediante diversas reformas normativas orientadas hacia la eliminación del soporte papel y la tramitación electrónica del procedimiento. El concepto de “*papel cero*” al que se refiere la catedrática DÍAZ PITA ha acompañado de forma paralela al reconocimiento de la prueba digital como categoría jurídica. Sin embargo, este esfuerzo normativo no ha ido acompañado de una regulación sistemática y unívoca de la denominada prueba digital por lo que presenta múltiples aristas y puntos de partida y de destino muy dispares<sup>4</sup>.

Uno de los problemas es la ausencia del concepto uniforme de “*prueba electrónica*” habiéndose adoptado distintas denominaciones como prueba digital, prueba electrónica, prueba informática o prueba tecnológica. No obstante, la controversia en torno a la prueba digital tiene su origen y antecedente histórico cuando se planteó que los medios de reproducción de palabra, la imagen y el sonido, pese a su uso, carecían de reconocimiento expreso como hechos probatorios atendiendo al *numerus clausus* de la enumeración de los medios de prueba del artículo 578 de la LEC de 1881 y del artículo 1217 del Código Civil<sup>5</sup>. La situación fue superada por la doctrina del Tribunal Supremo y la Ley de Enjuiciamiento Civil de 2000 al reconocerlos expresamente como medios de prueba aptos para fundamentar las pretensiones en el proceso civil<sup>6</sup>.

No hay una nomenclatura legal general siendo que la procesalista SANCHÍS CRESPO entenderá los medios probatorios electrónicos como “*aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal*”<sup>7</sup>, abogando por definirlos en función del soporte en el mismo sentido que el magistrado DELGADO MARTÍN considera que “*por prueba digital o electrónica cabe entender toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio. En esta definición cabe destacar los siguientes*

---

<sup>4</sup> Díaz Pita, M.<sup>a</sup> P., “Digitalización de la Justicia: prevención, investigación y enjuiciamiento”, en *Estudios*, 1ª edición, Aranzadi, Navarra, 2022.

<sup>5</sup> Delgado Martín, J., “La prueba digital. Concepto, clases, aportación al proceso y valoración”, *Sección Ciberderecho, Diario La Ley*, n.º 6, 2017, p. 13.

<sup>6</sup> Montero Aroca, J., “Las cintas magnetofónicas como fuentes de prueba (Comentario a la Sentencia del Tribunal Supremo, Sala I, de 30 de noviembre de 1981”, *Poder judicial*, 1983-1, p.40, para quien el empleo de grabaciones magnetofónicas, vídeos, fotografías, películas, etc, en el proceso civil era, justamente, reflejo del derecho al uso de los medios de prueba pertinentes para la defensa tal y como proclama el art. 24 de la Constitución.

<sup>7</sup> Sanchís Crespo, C., “La prueba en soporte electrónico”, en AA.VV., *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, Thomson Reuters Aranzadi, Navarra, 2012, pp.713.

*elementos: 1. Se refiere a cualquier clase de información; 2. Que ha de ser producida, almacenada o transmitida por medios electrónicos; 3. Y que pueda tener efectos para acreditar hechos en el proceso abierto en cualquier orden jurisdiccional”<sup>8</sup>.*

Sin embargo, la denominación mayormente aceptada por la doctrina es la de “*prueba electrónica*”, definida por el magistrado DE URBANO CASTRILLO como aquella que “*se expresa mediante un soporte electrónico, de ahí su nombre, creado por los modernos instrumentos tecnológicos de la información*”, quedando dentro del concepto de prueba electrónica aquellos hechos probatorios “*creados directamente a través de la informática -así un correo electrónico- las que proceden de medios de reproducción o archivos electrónicos -vídeos, fax, fotografía digital...- y las que se presentan mediante instrumentos informáticos del tipo disquetes, pen-drives, bases de datos, etc*”<sup>9</sup>.

La doctrina adoptada por el TS en la Sentencia de fecha 7 de diciembre de 1979 admitió y consideró aptos estos elementos siempre que ofrecieran las debidas garantías: 1) Ser una prueba pertinente y útil; 2) Ser una prueba obtenida sin violentar derechos y libertades fundamentales; 3) Ofrecer las debidas garantías de autenticidad<sup>10</sup>. Ahora lo que se pretende mediante la aceptación de la prueba electrónica es adaptar la justicia al entorno digital, superando la histórica limitación de medios analógicos.

## 2. CLASIFICACIÓN DE LOS MEDIOS DE PRUEBA EN LA LEY DE ENJUICIAMIENTO CIVIL Y CRIMINAL

### 2.1 Medios de prueba en la Ley de Enjuiciamiento Civil

Los medios de prueba se configuran como las herramientas que permiten al Tribunal la apreciación sensible del objeto de la prueba. Según lo afirmado por ROSENBERG, “*el juez puede percibir mediante propia intuición o puede percibir a través de transmisión*”. En el primer caso, la percepción judicial es lograda a través de los sentidos del propio juez, como ocurre en el caso del reconocimiento judicial. En el segundo caso, los instrumentos serán las cosas o personas que transmiten al juez la percepción sensible del objeto de la prueba y es aquí donde entran en juego el documento, el testigo, el perito y en el caso de la evidencia electrónica, los mensajes o archivos digitales, resulta esencial los conocimientos del juez para comprender

---

<sup>8</sup> Delgado Martín, J., “La prueba digital. Concepto, clases...”, op. cit., p.13.

<sup>9</sup> De Urbano Castrillo, E., “La valoración de la prueba electrónica”, Tirant lo Blanch, Valencia, 2009, p. 47.

<sup>10</sup> Montero Aroca, J., “Las cintas magnetofónicas...”, op. cit., p. 40.

los mandatos, registros de actividad o la validez de los soportes electrónicos o la intervención de peritos que expliquen su validez<sup>11</sup>.

La LEC del año 2000 se limita a enumerar de forma ordenada y sistemática los medios de prueba, con la finalidad de dotar al proceso de la necesaria seguridad jurídica y previsibilidad, sin perjuicio de permitir la admisión de nuevos medios probatorios ante las nuevas realidades sociales y avances tecnológicos. No contiene ningún apartado dedicado a la “prueba electrónica o prueba digital” como medio de prueba autónomo, pero sí recoge una serie de normas generales sobre medios de prueba (art 299), reglas sobre determinados soportes o instrumentos tecnológicos (arts. 382 a 384) y sobre todo el régimen de prueba documental. Es decir, incorpora una cláusula flexible de admisión de otros instrumentos probatorios útiles.

En la práctica, nuestros Tribunales admiten la utilización de medios probatorios tales como las cintas videomagnéticas, las bases de datos, los discos duros de los ordenadores etc., acordes a la evolución socioeconómica producida, siempre que quede acreditada su autenticidad, integridad, autoría, trazabilidad y licitud como se expondrá en los siguientes capítulos<sup>12</sup>.

La doctrina ha planteado diversas clasificaciones de las distintas pruebas, como la que distingue entre pruebas reales y personales. Las pruebas reales se basan en objetos, documentos o soportes materiales como por ejemplo sucede en el reconocimiento judicial con la prueba documental o la prueba digital, mientras que las pruebas personales hacen referencia a cuando la fuente de prueba es una persona (como por ejemplo un interrogatorio de partes o la prueba testifical)<sup>13</sup>. Otra clasificación diferencia entre pruebas directas que acrediten de manera directa los hechos controvertidos y las indirectas que permiten inferir la existencia del hecho a partir de otros hechos probados<sup>14</sup>.

Encontramos otra distinción entre pruebas preconstituidas y pruebas practicadas en el acto del juicio. Las pruebas preconstituidas son todas aquellas pruebas que existen antes de que de lugar el proceso, es decir, las existentes antes de iniciarlo (ej: documentos como los contratos o

---

<sup>11</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, op. cit., pp. 223-225.

<sup>12</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, op. cit., p. 224.

<sup>13</sup> Consejo General del Poder Judicial, “La prueba en el proceso civil...”, op. cit., pp. 65-68.

<sup>14</sup> De Miranda Vázquez, C., “Prueba directa vs. prueba indirecta (Un conflicto existente)”, n.º 38, 2015, pp. 76–77.

correos electrónicos) y las practicadas en el acto del juicio tienen un origen posterior, en la práctica de la fase probatoria (Ej: interrogatorio de testigos o reconocimiento judicial)<sup>15</sup>.

## **2.2 Medios de prueba en la Ley de Enjuiciamiento Criminal**

Los medios de prueba en el proceso penal no se encuentran enumerados de forma cerrada en un único precepto, la LECRIM los regula detalladamente en su Libro II en relación a la fase de instrucción y en su Libro III en relación el juicio oral.

Podemos clasificar los medios de prueba entre los clásicos o tradicionales y los especiales, derivados de las nuevas tecnologías. Los medios de prueba tradicionales se practican para desvirtuar la presunción de inocencia como: a) la confesión o interrogatorio del acusado (arts. 385 a 409 en fase de instrucción y arts. 688 a 700 en el juicio oral); b) la prueba testifical, la declaración de personas que presenciaron los hechos o tienen conocimiento de ellos (arts. 410 a 450 en fase de instrucción y arts. 701 a 722 en el juicio oral); c) la prueba pericial que consiste en los informes de expertos sobre materias técnicas, científicas o artísticas (arts. 456 a 485 en fase de instrucción y arts. 723 a 725 en el juicio oral); d) la prueba documental, documentos escritos o archivos (arts. 726 y 727 en el juicio oral); e) la inspección ocular y el reconocimiento judicial consistentes en el reconocimiento directo por el juez del lugar del delito o de objetos relacionados (arts. 326 a 333); y f) el careo entre testigos o procesados (arts. 451 a 455 en fase de instrucción y art. 713 en el juicio oral).

Los medios de prueba especiales fueron introducidos recientemente para adaptar la ley a la era digital. Se regulan las diligencias de investigación dirigidas a la obtención de pruebas como la intervención de comunicaciones telefónicas y telemáticas en los arts. 588 ter a hasta 588 ter i; la captación de imágenes y sonidos en lugares públicos en el art. 588 quinquies a; y el registro de dispositivos de almacenamiento masivo en el art. 588 sexies a.

Debemos aclarar que se incluyen como “medios especiales” medidas de investigación tecnológica o diligencias de investigación, que practicadas con garantías dan lugar a pruebas digitales como conversaciones intervenidas, grabaciones de imágenes o documentos electrónicos.

---

<sup>15</sup> Garcimartín Montero, R., “Comentario al artículo 294 de la Ley de Enjuiciamiento Civil”, en *Comentario a la Ley de Enjuiciamiento Civil*, tomo I, Aranzadi, Navarra, 2011.

En conclusión, mientras la LEC regula los medios de prueba con una lista cerrada permitiendo la adaptación tecnológica, la LECRIM dispersa la regulación entre la instrucción y el juicio oral, combinando métodos clásicos con nuevos medios especiales tecnológicos. De este modo la LEC prioriza la clasificación de la prueba según su naturaleza y momento, mientras que la LECRIM se enfoca en la eficacia para averiguar los hechos.

### 3. PRINCIPIOS GENERALES Y FINALIDAD DE LA PRUEBA

Los principios generales de los medios de prueba derivan tanto de la Constitución como de la Ley de Enjuiciamiento Civil. El marco de los derechos constitucionales fundamentales se encuentra en el artículo 24 de la Constitución Española que actúa como “paraguas” protector de toda la actividad probatoria<sup>16</sup>.

El derecho a la utilización de los medios de prueba se constituye como un derecho de configuración legal. No se articula como un derecho absoluto a que se admitan todas las pruebas sino que se condiciona al cumplimiento de tres requerimientos como son la pertinencia (que la prueba se relacione con el objeto); la utilidad (apta para acreditar los hechos alegados); y legal (que se proponga en la forma y momento procesal adecuado). La denegación arbitraria de una prueba relevante produce indefensión y abre la vía al recurso de amparo ante el Tribunal Constitucional<sup>17</sup>.

La constitución reconoce el principio de licitud de la prueba que supone que no surtan efecto las pruebas obtenidas directa o indirectamente vulnerando derechos fundamentales y libertades públicas lo que resulta esencial en la prueba digital en cuando al modo de obtener una conversación o un vídeo grabado o el acceso a un documento que se encuentra en un dispositivo ajeno. Se consigna en el art. 11 LOPJ<sup>18</sup> que si una prueba es ilícita debe ser expulsada del proceso y no puede ser valorada por el juez. Otro principio rector es el de la presunción de inocencia que se resume en que la carga de la prueba corresponde a quien acusa, quien debe probar, no siendo el investigado quien deba demostrar la inocencia. Se exige que haya una

---

<sup>16</sup> Gómez Montoro, Á. J., “Capítulo II: Los derechos procesales del artículo 24 CE”, en Gómez Montoro, Á. J., *Jurisdicción constitucional y judicial en el recurso de amparo*, Tirant lo Blanch, Valencia, 2006.

<sup>17</sup> Díez-Picazo, L. (2008). *Sistema de Derechos Fundamentales*. Editorial Aranzadi, S.A.U.

<sup>18</sup> Artículo 11 de la Ley Orgánica 6/1985, de 1 de Julio, del Poder Judicial.

mínima actividad probatoria de cargo, lícita y con todas las garantías y en caso de duda, prevalece el principio *in dubio pro reo*<sup>19</sup>.

Derivados del derecho a la tutela judicial efectiva y al proceso con todas las garantías surgen los principios de contradicción e igualdad de armas. Ello implica que, si la contraparte no ha tenido la oportunidad de conocer, cuestionar y contraprobar una prueba, no puede ser valorada, y permite impugnar la prueba digital. De esta forma ambas partes tienen idénticas posibilidades de proponer y practicar pruebas. Si la Administración posee medios tecnológicos que la defensa no pueda replicar o conocer, se rompe el equilibrio constitucionalmente exigido<sup>20</sup>.

La Constitución reconoce el principio de publicidad e inmediación en el art. 120 CE y con ello surge la exigencia de que las actuaciones judiciales sean públicas, salvo excepciones tasadas. Aunque no se recoge de forma expresa la exigencia del proceso con todas las garantías, implica que el juez que resuelva haya presenciado la práctica de la prueba directamente. La exigencia de la libre valoración de la prueba se reconoce como otro principio general que supone que no hay un valor tasado para valorar pruebas, por lo que el juez es libre siempre que no caiga en la arbitrariedad. Derivado de este principio, surge el de motivación de las resoluciones judiciales que se reconoce en el art. 120 CE y que exige que se justifique por qué dar validez a una prueba frente a otra<sup>21</sup>.

La LEC desarrolla los principios constitucionales en diversos artículos del texto legal, así del artículo 299 LEC se deduce el principio de legalidad al recoger los medios de prueba que son admisibles incluyendo cualesquiera que sean útiles y no estén prohibidos por lo que se admite la prueba digital, aquella que contiene una información que se encuentra incluida en un medio electrónico o es transmitida por él<sup>22</sup>.

El principio de pertenencia y utilidad está recogido en el artículo 283 LEC al declarar que sólo se admitirán aquellas pruebas que guarden relación con el objeto del proceso y sean relevantes y útiles para esclarecer los hechos. El principio de inmediación deriva de los artículos 137 y

---

<sup>19</sup> Díez-Picazo Giménez, L.M., “Sistema de Derechos Fundamentales”, Civitas, Madrid, 2008.

<sup>20</sup> Garrido Carrillo, F. J., *Principios y garantías del proceso penal de menores*, Aranzadi, Navarra, 2023.

<sup>21</sup> González Granda, P., “La valoración de la prueba”, en Romero Pradas, S. y González Cano, M. I. (coords.), *La prueba*, Aranzadi, 2017.

<sup>22</sup> Orellana Cano, N. A., “La prueba en el tráfico mercantil”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 50, Madrid, 2009, pp. 26-30

289 LEC por lo que la presencia judicial será inexcusable, así como también en las rectificaciones o ampliaciones de los dictámenes periciales. El artículo 138 LEC enuncia el principio de publicidad de las actuaciones judiciales salvo excepciones.

El principio de libre valoración puede inferirse de los artículos 316 y 348 LEC ya que se prevé que sea el Juez quien habrá de examinar y valorar por sí mismo la prueba conforme a las reglas de la sana crítica. Los arts. 285, 287 y 429 LEC recogen el principio de contradicción conforme al cual toda prueba propuesta y practicada debe ser conocida por todas las partes involucradas y susceptible de su sometimiento a discusión. Relacionado con este principio, se encuentra el principio de igualdad de armas.

En conclusión, la prueba es el puente entre los hechos y la sentencia. Los principios generales aseguran su solidez (principio de legalidad), su transparencia (principio de publicidad), su equilibrio (igualdad de armas y contradicción) y su humanidad (principio de inmediación y de respeto de los derechos fundamentales).

## **CAPÍTULO II. LA PRUEBA ELECTRÓNICA Y SU ENCAJE EN EL ORDENAMIENTO PROCESAL, NATURALEZA DE LOS DOCUMENTOS ELECTRÓNICOS Y FIRMA DIGITAL**

### **1. LA PRUEBA ELECTRÓNICA Y SU ENCAJE EN EL ORDENAMIENTO PROCESAL**

La prueba electrónica o digital comprende el conjunto de herramientas e instrumentos que permiten archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas, incluyendo correos electrónicos, mensajes de mensajería instantánea, páginas web, bases de datos, documentos electrónicos, grabaciones de audio y vídeo y otros soportes digitales.

Del apartado 2º del artículo 299 se pueden diferenciar distintos tipos de prueba digital o electrónica<sup>23</sup> como documentos electrónicos (emails, chats, archivos digitales, páginas webs y redes sociales), medios de reproducción de imagen y sonido (incluyendo vídeos, audios), instrumentos informáticos (registros de datos, hojas de cálculo, discos duros...) y la prueba

---

<sup>23</sup> Abel Lluch, F. J., “El documento electrónico: acceso, impugnación y valoración” en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 46, Madrid, 2022, p.8

pericial informática como medio para garantizar la autenticidad. El apartado tres permite incluir cualquier otro medio de prueba no mencionado del que pueda obtenerse certeza sobre los hechos relevantes, en cuyo caso, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que resulten necesarias.

Las pruebas digitales pueden clasificarse en distintos grupos en atención a su origen y naturaleza como son los documentos electrónicos que incluyen cualquier archivo digital que contenga información relevante para un caso, correos electrónicos, mensajes de texto y aplicaciones de mensajería instantánea, registros de navegación en internet como el historial de navegación y cookies entre otros, redes sociales (Twitter, Instagram, Facebook etc.) y datos de dispositivos electrónicos respecto a información almacenada en computadoras, teléfonos móviles y tabletas entre otros<sup>24</sup>.

La prueba documental electrónica constituye la manifestación más tradicional de la prueba digital. En el proceso, se puede distinguir un doble acceso, el primero como documento privado siendo lo más habitual en la práctica y el segundo como documento público, pero menos frecuente debido al coste económico que supone la intervención de un notario<sup>25</sup>.

En el primer caso, si la página web o correo electrónico entre otros tipos de medios de prueba documental no se impugnan, tendrán el valor de prueba plena y su eficacia se extenderá al hecho, pero si por el contrario dicha página o correo se impugnan, su eficacia probatoria se valorará conforme a las reglas de la sana crítica del artículo 326 LEC necesitando una prueba pericial en tal caso para reconocer su autenticidad. En el caso de acceso como documento público, cabrá solicitar un acta de protocolización o de presencia notarial para dar fe del contenido de la prueba documental<sup>26</sup>.

El principio general establece que sólo aquellos documentos auténticos producirán plena eficacia probatoria independientemente del soporte en que se encuentren<sup>27</sup>. Sin embargo, no toda prueba digital revestirá naturaleza documental, puesto que sólo tendrá tal consideración cuando tenga naturaleza de documento y en los restantes casos en los que el contenido de la

---

<sup>24</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, op. cit., pp. 225–226.

<sup>25</sup> Abel Lluch, F. J., “El documento electrónico...”, op. cit., pp. 6–7.

<sup>26</sup> Id.

<sup>27</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, op. cit., pp. 275–279.

prueba consista en medios de reproducción de imagen o sonido, será aplicable el artículo 382 LEC, debiendo valorarse por el juez conforme a las reglas de la sana crítica.

En estos supuestos del artículo 382 LEC hay que prestar atención a la posible colisión entre derechos fundamentales, en concreto, entre el derecho a la tutela judicial efectiva del artículo 24 de la Constitución Española y el derecho a la intimidad y a la propia imagen. La admisión de la legalidad de las grabaciones de imagen y sonido ha sido condicionada por la jurisprudencia a que su obtención haya sido realizada sin vulneración de derechos fundamentales<sup>28</sup>.

En cuanto al valor probatorio de estas reproducciones, el apartado 3º del artículo 382 remite a las reglas de la sana crítica, la misma norma que establece para la prueba testifical en el artículo 376. El artículo 384 LEC establece que la aportación de los distintos tipos de prueba al proceso es válida siempre que las partes pongan a disposición del juez los medios necesarios para su reproducción. Evidentemente, deberá respetarse las normas sobre el momento de proposición de la prueba, que en el caso civil será en el procedimiento declarativo ordinario en la Audiencia Previa como se recoge en el art. 429.1 LEC y en la vista, en el procedimiento declarativo verbal conforme al art. 443 LEC.

Por otra parte, la prueba pericial informática es un elemento clave del proceso para garantizar la autenticidad, integridad y no manipulabilidad de la prueba electrónica, en especial cuando la misma es impugnada. Dicho elemento probatorio resulta de gran relevancia cuando se habla de la prueba electrónica cuyo origen proviene de las redes sociales y plataformas digitales. La prueba pericial tiene como finalidad acreditar el verdadero origen de la comunicación, la identidad de los interlocutores y la integridad de su contenido<sup>29</sup>.

En la STS de 1 de julio de 2025 relativa a unos mensajes de WhatsApp, se resolvió que no es imprescindible la prueba pericial informática en todos los supuestos si existen otros elementos que acrediten dicha autenticidad. En este sentido, la STS 754/2015 de 27 de noviembre<sup>30</sup>, aclara que no basta con una impugnación genérica para exigir la pericial si la prueba es coherente y

---

<sup>28</sup> Rivas Velasco, M. J., “Documento electrónico: medios e instrumentos de reproducción de la palabra, sonido e imagen”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 24, Madrid, 2018, pp. 9-12.

<sup>29</sup> Consejo General del Poder Judicial, “La prueba en el proceso civil...”, op. cit., pp. 29-32.

<sup>30</sup> Sentencia del Tribunal Supremo, Sala de lo Penal, núm. 754/2015, de 27 de noviembre (versión electrónica-base de datos VLEX). Fecha de última consulta: 1 de febrero de 2026.

se ha aportado además al proceso el soporte original y no existen indicios objetivos de manipulación.

En función de lo anterior, queda claro que la prueba pericial no es obligatoria en todos los casos ya que el juez podrá entrar a valorar los medios probatorios si cuenta con otros elementos suficientes que garanticen la corroboración de su integridad y autenticidad. Sin embargo, sí que será necesaria cuando se impugne por la otra parte cuestionándose la autenticidad, integridad y manipulabilidad del hecho probado. La prueba pericial en estos casos, resulta necesaria que sea realizada por un profesional del ámbito, esto es, de un perito informático o ingeniero de telecomunicaciones, ya que el propio tribunal carece de conocimientos técnicos suficientes para entrar a valorar la prueba digital por sí mismo<sup>31</sup>.

Por otro lado, se pueden destacar dos formas de acceso de la pericia al proceso: el acceso a modo de prueba pericial instrumental y el acceso como medio probatorio autónomo. Con respecto al primer tipo de clasificación, el acceso a modo de prueba pericial instrumental, es importante entender que el informe pericial no es la principal prueba, sino que hay una actividad probatoria que necesita el apoyo de una pericial para verificar su autenticidad. Así pues, su función radica en ayudar a comprender la prueba electrónica, a comprobar si es auténtica y verificar si ha sido o no manipulada. La pericial puede tener su origen ante la impugnación del medio probatorio por su falta de autenticidad o integridad<sup>32</sup>.

En el segundo caso, en el acceso como medio probatorio autónomo, la prueba la constituye el informe pericial, es decir, no hay ningún documento previo a analizar por el perito, sino que es el experto el único que puede obtener dicha información precisando conocimientos informáticos específicos. Esto sucede para averiguar por ejemplo el número de visitas que ha recibido una página web<sup>33</sup>. La parte acompaña junto a las alegaciones un dictamen pericial o en su caso solicitar la designación judicial del perito informático (Art 339.2 LEC). En conclusión, sea como pericial autónoma o pericial instrumental, ambos tipos son modalidades de prueba pericial, sujeto a la Ley de Enjuiciamiento Civil. La prueba electrónica no es un medio aislado, sino una realidad tecnológica que se integra en el proceso judicial a través de

---

<sup>31</sup> Consejo General del Poder Judicial, “La prueba en el proceso civil...”, op. cit., pp. 30–33.

<sup>32</sup> Consejo General del Poder Judicial, “La prueba en el proceso civil...”, op. cit., pp. 9-12.

<sup>33</sup>Id.

diversas vías. Su eficacia depende de un equilibrio entre su aportación técnica y el respeto a los derechos y garantías procesales.

## 2. NATURALEZA JURÍDICA DE LOS DOCUMENTOS ELECTRÓNICOS

El documento electrónico es aquel que está recogido en un soporte electrónico (conteniendo información y datos almacenados en un CD, DVD o disco duro.) que incorpora datos y que está firmado electrónicamente<sup>34</sup>.

Conforme al artículo 3.10 del Reglamento eIDAS, aplicable en España vía Ley 6/2020, se entiende como firma electrónica *“Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica o funcionalmente a otros datos electrónicos, utilizados por el firmante como medio de firma”*<sup>35</sup>. Se trata de una herramienta que cumple con funciones de identificación inequívoca del firmante, aseguramiento de la integridad del documento firmado y demostración del carácter único de los datos utilizados por el mismo<sup>36</sup>.

Se pueden distinguir dos tipos de firma electrónica: avanzada y reconocida. La avanzada permite identificar al firmante y la detección de cualquier posterior cambio de los datos firmados, mientras que la reconocida está basada en un certificado reconocido y generado mediante un dispositivo seguro de creación de firma<sup>37</sup>.

Los documentos electrónicos pueden serlo en sentido estricto (memoria RAM), permanentes (disquetes), inalterables (CD) o en sentido amplio que son las copias en soporte externo del documento<sup>38</sup>. Podrán servir de soporte de documentos públicos, administrativos o privados, gozando de idéntica eficacia jurídica y procesal que los documentos en papel<sup>39</sup>. Al procedimiento procesal lo que realmente le resulta relevante es el objeto de la actividad

---

<sup>34</sup> Rivas Velasco, M. J., “Documento electrónico...”, *op. cit.*, pp. 3–5

<sup>35</sup> Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DOUE 28 de agosto de 2014).

<sup>36</sup> García Martín, J. A. et al., “Administración electrónica. Aspectos jurídicos organizativos y técnicos”, Thomson Reuters Aranzadi, Navarra, 2021, p. 2.

<sup>37</sup> Rivas Velasco, M. J., “Documento electrónico...”, *op. cit.*, p. 3.

<sup>38</sup> Urbano Castrillo, E. de y Torres Morato, M. A., *La prueba ilícita penal: estudio jurisprudencial*, Aranzadi, Navarra, 2003, pp. 47.

<sup>39</sup> Alemany Eguidazu, J., “La prueba de la autenticidad electrónica con la LEC”, *Poder Judicial. Nueva Época*, n.º 1, 2002, cap. III, apartado 2 (Medios probatorios con la nueva Ley de Enjuiciamiento Civil).

probatoria, siendo este el documento electrónico, no el soporte que sirve como medio material o técnico cuya finalidad es almacenar o contener al documento. Así, como ejemplo, en un procedimiento lo que se va a probar no va a ser el terminal del teléfono móvil, sino los mensajes, audios o vídeos que están contenidos en él. El soporte electrónico no constituye una prueba como tal<sup>40</sup>.

Debe tenerse en cuenta que los documentos electrónicos no exigen para su existencia de un soporte físico (por ejemplo, archivos) si bien para que puedan hacer prueba en juicio es necesario que se materialicen de alguna forma en el proceso. Así, si se trata de medios audiovisuales se necesitará el soporte original correspondiente, pero si se trata de medios informáticos, deberá aportarse un CD o disco ante la imposibilidad de aportar el ordenador. Si el documento electrónico está firmado digitalmente, habrá de aportarse el certificado de la entidad certificadora<sup>41</sup>.

La firma electrónica avanzada o cualificada refuerza el valor probatorio del documento electrónico, otorgando un efecto jurídico al de una firma manuscrita en papel<sup>42</sup>. Sus efectos probatorios se regirán según lo dispuesto en el Reglamento eIDAS. En caso de impugnación de la autenticidad de la firma, será de aplicación el artículo 326.4 LEC<sup>43</sup>.

En relación con la impugnación documental, si cuestiona la autenticidad del documento electrónico, la parte que lo haya propuesto como alegación deberá proponer otro medio de prueba, en relación con el apartado 2º del artículo 326 (prueba complementaria). La prueba complementaria no sustituye a la prueba principal, sino que únicamente la corrobora o apoya para demostrar su veracidad<sup>44</sup>. Un ejemplo de ello es cuando una de las partes impugna un correo electrónico alegando posible manipulación y la contraparte debe presentar una pericial informática acreditando el origen y la fecha exactos y la integridad del mensaje.

---

<sup>40</sup> Delgado Martín, J., “Estándares probatorios en la prueba digital”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 46, Madrid, 2022, p. 10.

<sup>41</sup> Ibid., pp. 30–35.

<sup>42</sup> Urbano Castrillo, E. de y Torres Morato, M. A., “La prueba ilícita penal...”, *op. cit.*, pp. 47.

<sup>43</sup> Delgado Martín, J., “Estándares probatorios...”, *op. cit.*, pp. 30–34.

<sup>44</sup> Abel Lluch, F. J., “El documento electrónico...”, *op. cit.*, pp. 8–10.

### CAPÍTULO III. OBJETO DE LA PRUEBA, DIFICULTADES EN EL ACCESO A LA MISMA, VALORACIÓN JUDICIAL Y CADENA DE CUSTODIA

#### 1. OBJETO DE LA PRUEBA Y DIFICULTADES E ILICITUD EN EL ACCESO A LA MISMA

El artículo 281 LEC define el objeto de la prueba como *aquellos hechos controvertidos que guarden relación con el objeto del proceso y no gocen de notoriedad absoluta y general*. Además, formarán parte del objeto las costumbres no discutidas entre las partes y el derecho extranjero. En la STS 344/2016 de 3 de febrero de 2016, de 27 de septiembre<sup>45</sup>, entiende que los hechos que gozan de notoriedad absoluta y general son aquellos datos económicos y públicos y de libre acceso que han sido objeto de una amplia difusión y conocimiento general<sup>46</sup>.

En correspondencia con las fases de la prueba digital en un proceso, la primera etapa de obtención de la prueba implica la *recopilación de los datos* o información generados o almacenados en soportes electrónicos. Para ello, es fundamental que las partes del proceso accedan a dicha información de forma lícita, garantizando la protección de derechos fundamentales como la intimidad, la libertad de expresión, el secreto de las telecomunicaciones y la protección de los datos personales (art.18.4 CE). Si, por el contrario, se vulnera cualquiera de estos derechos, la prueba obtenida se considerará ilícita<sup>47</sup>. Un ejemplo paradigmático es la STS del 28 de abril de 2011 en la que el Tribunal señaló que la obtención de documentos privados sin consentimiento puede constituir una vulneración del derecho fundamental a la intimidad, lo que determinaría la ilicitud de la prueba<sup>48</sup>.

En cuanto al *acceso a los datos*, este dependerá de la específica fuente probatoria. Por ello, se pueden distinguir distintos tipos de acceso: acceso a dispositivos electrónicos, acceso a redes sociales o aportación de datos propios como correos electrónicos o mensajes de WhatsApp, entre otros<sup>49</sup>. Ejemplo: dos personas se ponen de acuerdo en un contrato por WhatsApp, la

---

<sup>45</sup> Sentencia de la Audiencia Provincial de Madrid, Sección 25.ª, núm. 344/2016, de 27 de septiembre (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 5 de febrero de 2026.

<sup>46</sup> Consejo General del Poder Judicial, “La prueba en el proceso civil...”, *op. cit.*, p. 3.

<sup>47</sup> Delgado Martín, J., “Estándares probatorios...”, *op. cit.*, pp. 6–7.

<sup>48</sup> Sentencia del Tribunal Supremo, Sala Primera, núm. 275/2011, de 28 de abril (recurso núm. 1083/2007) (versión electrónica-base de datos del Tribunal Supremo). Fecha de última consulta: 7 de febrero de 2026.

<sup>49</sup> Delgado Martín, J., “Estándares probatorios...”, *op. cit.*, pp. 6–7.

fuente probatoria es la aplicación de mensajería instantánea y lo que se prueba son los respectivos mensajes constitutivos del contrato vinculante.

Por lo general, los documentos electrónicos acceden al proceso por el cauce de la prueba documental, pero ello no impide que puedan hacerlo a través de distintos medios de prueba. En lo que concierne a la prueba documental, se podrá distinguir un doble acceso tanto como documento público como privado. El documento público, en la realidad práctica, es menos frecuente debido al coste en algunos casos elevado del notario, mientras que el privado será el documento mayormente utilizado en la práctica forense<sup>50</sup>.

Finalizada la fase de obtención de los datos a través de una fuente digital, se procede a la incorporación de dichos datos al proceso y, para ello, se exigirá la concurrencia de tres requisitos: pertinencia, necesidad e ilicitud, desarrollados en un epígrafe ulterior<sup>51</sup>.

En el proceso civil y a modo de diferenciación de lo que sucede en el ámbito penal, el principio de aportación de cada parte determina que cada una deberá elegir las pruebas que consideren útiles y pertinentes para el proceso, además del método de obtención de las fuentes de prueba. En el ámbito de las pruebas digitales, el acceso a las mismas a través de las fuentes puede presentar una mayor dificultad por la razón de que las fuentes abiertas al público como por ejemplo las redes sociales o páginas web serán más fáciles de obtener que las que tienen el carácter privado y tienen limitado el acceso a unas personas concretas (ejemplo: será mucho más difícil acceder a pruebas que se encuentren en el ordenador de la contraparte o de un tercero o servidores ajenos)<sup>52</sup>.

Bien es cierto que la LEC no ofrece una solución legal o un procedimiento para el caso de que los datos electrónicos se encuentren en poder de la contraparte o de terceros. Es por ello, que esta “laguna” se soluciona mediante “mecanismos puntuales de tutela anticipatoria”, es decir, mediante herramientas legales para conseguir pruebas antes del inicio del juicio, tal y como establece el magistrado Joaquín Delgado Martín<sup>53</sup>. Estas herramientas consisten en practicar las diligencias preliminares *numerus clausus* recogidas en los artículos 256 a 263 LEC que

---

<sup>50</sup> Abel Lluch, F. J., “El documento electrónico...”, *op. cit.*, p. 6.

<sup>51</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, *op. cit.*, pp. 275–276.

<sup>52</sup> Delgado Martín, J., “Estándares probatorios...”, *op. cit.*, pp. 7–10.

<sup>53</sup> *Ibid.*, pp. 6–7.

consisten en actuaciones previas al proceso para obligar a alguna de las partes en cuyo poder se encuentren las pruebas pertinentes al proceso a entregar o mostrar dichos documentos ante el Juez.

Por otra parte, aunque la LEC en tales artículos no hace referencia expresamente a documentos electrónicos, se puede realizar una interpretación extensiva conforme al artículo 3.1 del Código Civil e incluir en la misma dentro del concepto de documentos aquellos que se encuentren en soporte digital<sup>54</sup>. Así, pese a las limitaciones que impone la regulación para el acceso a pruebas en poder de terceros o de la contraparte, dichas pruebas se pueden obtener a través de los mecanismos excepcionales mencionados antes.

Las pruebas ilícitas son aquellas que se han obtenido vulnerando los derechos fundamentales en especial el derecho a la intimidad y el derecho al secreto de las telecomunicaciones. La nulidad de las pruebas se extiende a todas aquellas pruebas con las que exista una conexión de antijuridicidad y podrá ser apreciada bien de oficio por el Juez o solicitada por la parte que esté legitimada<sup>55</sup>. Como regla general ordinaria, la aportación de las pruebas por las partes debe tener lugar en el momento de la demanda y de la contestación, siguiendo lo establecido en el artículo 265 LEC con la finalidad de que la contraparte pueda preparar debidamente su defensa.

Excepcionalmente, se procede a la admisión de nuevas pruebas en la audiencia previa de acuerdo con los casos del art 270 LEC cuando la parte justifique que no le fue posible aportarlas con anterioridad, debido a que no tiene acceso a ellas en el momento de interponer la demanda o formular la contestación. Un ejemplo aplicado a las pruebas digitales supondría que los emails están en el servidor de la empresa demandada y por consiguiente el demandante no tenía acceso a dicha cuenta. Es por lo que, en la audiencia previa, el demandante debe solicitar la admisión de nuevos correos electrónicos obtenidos mediante diligencias preliminares<sup>56</sup>.

La prueba digital debe aportarse en soporte adecuado ajustándose a la normativa sobre el expediente judicial electrónico. La necesidad del traslado a la parte contraria constituye un requisito esencial para garantizar la contradicción y la igualdad de armas. Tras la reforma de la LEC, se permite la aportación de documentos públicos por copia simple en soporte electrónico

---

<sup>54</sup> Id.

<sup>55</sup> Ibid., p. 8.

<sup>56</sup> Ibid., p. 11.

a través de imagen digitalizada incorporada como anexo que ha de ir firmado mediante firma electrónica reconocida.

Los documentos privados como un correo electrónico si no se impugnan por la parte contraria o si por el contrario se reconocieran por la misma, tienen el valor de prueba plena según lo establecido en el artículo 326.1 LEC y su eficacia se extiende al hecho, acto, fecha en que se ha producido dicha documentación y las personas intervinientes (Art. 319.1 LEC). Si por el contrario se impugnasen, dicha prueba será valorada por el juez conforme a las reglas de la sana crítica y pudiendo llegarse a proponer una pericial para acreditar su autenticidad. Para el acceso a los documentos públicos será requisito imprescindible para su correcta incorporación al proceso la solicitud de un acta de protocolización o de presencia notarial para dar fe del contenido de la prueba.

Los documentos privados, pueden presentarse por medio de imágenes digitalizadas incorporadas a anexos firmados electrónicamente, pudiendo presentarse la copia simple siempre que no se impugne y deben aportarse siempre tantas copias de los documentos informáticos como partes haya en el proceso (Arts 273 LEC). En el caso de los documentos electrónicos públicos pueden aportarse en original electrónico o por copia en papel o digitalizada<sup>57</sup>. Finalmente, en el caso de que se haya incorporado correctamente la prueba al proceso, procede la valoración de la misma bajo los criterios de libre valoración<sup>58</sup>.

## 2. VALORACIÓN JUDICIAL, CARGA DE LA PRUEBA Y GARANTÍAS DE AUTENTICIDAD

En lo que respecta a la práctica de la prueba, debe realizarse de forma contradictoria, permitiendo a las partes alegar sobre su autenticidad y exactitud. El juez procede a su valoración conforme a las reglas de la sana crítica, teniendo en cuenta la posible manipulación y la existencia de complementarias.

La carga de la prueba, según el artículo 217 LEC en sus apartados 2 y 3, establece que corresponde al actor y al demandado reconviniendo la carga de probar los hechos de los que

---

<sup>57</sup> Ibid., p. 16.

<sup>58</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, op. cit., pp. 225–226.

ordinariamente se desprenda. Por tanto, le incumbe al demandado acreditar los hechos impositivos, extintivos o excluyentes que neutralicen su eficacia jurídica (art. 217.3 LEC).

En el caso de la valoración de los documentos electrónicos privados, si se impugna la autenticidad de un documento, la parte que lo aportó debe demostrar su veracidad e integridad mediante otro medio de prueba. Si no, el juez procede a examinar la prueba conforme a las reglas de la sana crítica<sup>59</sup>. En relación con la valoración de la prueba, la Audiencia Provincial de Baleares en su Sentencia núm. 352/2012 de 23 de julio, establece que “*dentro de las facultades concedidas al efecto a Jueces y Tribunales, estos pueden conceder distinto valor a los medios probatorios puestos a disposición e incluso, optar entre ellos por el que estime más conveniente y ajustado a la realidad de los hechos*”<sup>60</sup>.

Si, por el contrario, resulta acreditada su autenticidad, las costas, gastos y derechos que origine el cotejo serán de cargo de quien hubiese formulado la impugnación<sup>61</sup>. Respecto a los documentos electrónicos públicos, si son impugnados, se procederá a su cotejo con el original, que puede realizar el tribunal directamente, manteniéndose su eficacia probatoria si se acredita su correspondencia<sup>62</sup>.

Cuando la prueba se presente en un soporte electrónico, resulta necesaria su práctica para acceder a su contenido, la cual debe realizarse en un lugar distinto del Tribunal con el fin de garantizar la correcta comprobación de su autenticidad. Entre los requisitos y garantías para la práctica y la valoración de la prueba digital, deben salvaguardarse la autenticidad, la integridad, la posibilidad de contradicción y respetar los derechos fundamentales. El órgano judicial debe valorar la proporcionalidad y necesidad cuando la prueba afecte a estos derechos.

La autenticidad de la prueba digital es un aspecto fundamental en el proceso, dada su posible y fácil manipulación. Por tanto, si la parte no impugna la autenticidad, la prueba será plena (art. 326.1) y el juez entonces procede conforme a las reglas generales. La facilidad de la manipulación de las pruebas digitales ha venido de la mano de la Sentencia del Tribunal

---

<sup>59</sup> Tapia Fernández, I., “Comentario al artículo 217 de la Ley de Enjuiciamiento Civil”, en *Comentarios a la Ley de Enjuiciamiento Civil*, colección Grandes Tratados, Aranzadi, Navarra, 2001.

<sup>60</sup> Sentencia de la Audiencia Provincial de Baleares, Sección 5.ª, núm. 352/2012, de 23 de julio (recurso núm. 187/2012) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 8 de febrero de 2026.

<sup>61</sup> Delgado Martín, J., “Estándares probatorios...”, *op. cit.*, p. 17.

<sup>62</sup> *Id.*

Supremo 300/2015 de 19 de mayo <sup>63</sup> afirmando que la “*manipulación es un rasgo distintivo de las pruebas digitales y tecnológicas formando parte de la realidad de las cosas. El anonimato y la libre creación de cuentas con una identidad fingida hacen perfectamente posible aparentar una comunicación*”<sup>64</sup>.

Una prueba digital se considera válida cuando cumple determinados requisitos, entre ellos que su obtención haya sido lícita, que sea auténtica e íntegra (no alterada) y que se cumpla la regla de la cadena de custodia.

### 3. LA CADENA DE CUSTODIA

La doctrina de la cadena de custodia, consolidada por la jurisprudencia del TS y del TC, responde a la necesidad, de adoptar todas las precauciones necesarias para garantizar que las pruebas lleguen al juicio tal como fueron recogidas o presentadas, asegurando que no hayan sufrido manipulación o alteración alguna<sup>65</sup>. Una de las definiciones más utilizadas en la literatura jurídica española para la cadena de custodia aparece en la STS 1190/2009<sup>66</sup>, de 3 de diciembre, en la que se indica que la conservación de la cadena de custodia satisface la garantía de la «mismidad de la prueba»<sup>67</sup>.

El procesalista ARBÓS Y LLOBET defienden que el documento electrónico no tiene una presentación material, puesto que consiste en una información preservada en forma electrónica. Por ello, el problema de la conservación no radica sólo en la pervivencia del soporte físico, sino que está relacionado con el hardware y software consustanciales para su reproducción. Uno de los aspectos vinculados con la conservación de los contenidos será la capacidad de

---

<sup>63</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 300/2015, de 19 de mayo (versión electrónica-base de datos VLEX). Fecha de última consulta: 8 de febrero de 2026

<sup>64</sup> Tardón Olmos, M., “La violencia de género a través de las nuevas tecnologías”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 37, Madrid, 2017, pp.17,18.

<sup>65</sup> Ortuño Navalón, M.ª del Carmen (2014). *La prueba electrónica ante los tribunales*, Tirant lo Blanch

<sup>66</sup> Sentencia del Tribunal Supremo, Sala Primera, núm. 1190/2009, de 3 de diciembre (versión electrónica-base de datos VLEX). Fecha de última consulta: 9 de febrero de 2026.

<sup>67</sup> Rubio Alamillo, J., “Conservación de la cadena de custodia de una evidencia digital”, *Diario La Ley*, n.º 8859, 9 de noviembre de 2016, Wolters Kluwer, Madrid, p. 3 (disponible en <https://peritoinformaticocolegiado.es/wp-content/uploads/Conservacion-de-la-cadena-de-custodia-de-una-evid....pdf>; última consulta 1/03/2026).

duración de los soportes (CD, DVD, etc.) donde radican los archivos digitales y otro será la disponibilidad de mecanismos o lenguajes que permitan acceder a la información<sup>68</sup>.

La evolución tecnológica tiene como consecuencia la obsolescencia de mecanismos y formatos de almacenamiento, por lo que ya no existen sistemas actuales para recuperarlos. Por eso, es importante transferir la información a soportes compatibles con la tecnología vigente y para ello, existen en la actualidad varios métodos como el uso de claves de seguridad, códigos de acceso encriptados y antivirus<sup>69</sup>.

Todo lo anterior aplicado al ámbito de la prueba digital, englobaría todas las actuaciones técnicas y documentales destinadas a garantizar que una evidencia digital se mantenga inalterada desde su obtención hasta su valoración judicial. Su única finalidad radica en convencer al juez de que su contenido es auténtico e íntegro<sup>70</sup>.

Además, permite conocer el momento exacto en el que se acceden a los datos concretos, la identidad de la persona que accede y la forma en la que se conserva. Se configura como un principal instrumento técnico-procesal para acreditar la autenticidad de la prueba. En nuestro país, las únicas figuras de fedatarios públicos existentes son el Notario y el Letrado de la Administración de Justicia, de modo que son estos los que mediante el documento público den fe del proceso de custodia y por consiguiente, la salvaguarda de la integridad de la prueba para proceder a su posterior análisis.

La conservación de la cadena de custodia en un disco duro o memoria de almacenamiento masivo es una cuestión delicada. La contaminación resulta bastante probable solamente mediante la mera conexión de un disco duro o memoria USB a un ordenador personal para proceder a su análisis, sin necesidad de interactuar con el disco. Para evitar que ocurra esto, es imprescindible el uso de bloqueadoras de escritura, que son dispositivos que actúan como

---

<sup>68</sup> ARBÓS Y LLOBET, RAMÓN. "Conservación del documento electrónico". En "La Prueba Electrónica", op. colec. Abel Lluch, Xavier y Picó i Junoy, Joan (dirs.). Colección de Formación Continua Facultad de Derecho ESADE. Serie Estudios prácticos sobre los medios de prueba. Bosch edit. 2011, págs. 348 y ss.

<sup>69</sup> Ortuño Navalón, M.<sup>a</sup> del Carmen, "Aspectos procesales de la prueba electrónica", en Ortuño Navalón, M.<sup>a</sup> del Carmen, *La prueba electrónica ante los tribunales*, Tirant lo Blanch, Valencia, 2014.

<sup>70</sup> García Pérez, M. F., "Nuevas tecnologías y derechos humanos: análisis de las grabaciones en el proceso penal", en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 19, Madrid, 2022, pp. 29-31.

puede entre el disco duro o memoria y el ordenador, de tal forma que el disco o memoria nunca se conecta directamente al ordenador<sup>71</sup>.

En el caso de que se presente un escenario de registro domiciliario, será el LAJ quien se ocupa de precintar los dispositivos intervenidos con el único fin de supervisar que los precintos se mantengan inalterados una vez finalizado el análisis directo del contenido de los mismos o su volcado o clonado. Cuando en sede judicial se decreta la imposibilidad de realizar el volcado, cabe la posibilidad de depositar los dispositivos en manos de la policía, pudiendo realizar el análisis incluso sin intervención del Letrado de Administración de Justicia<sup>72</sup>.

La cadena de custodia debe estar presente cuando se lleve a cabo cualquier pericial informática respecto de las fuentes de información a analizar, en cada caso: correo electrónico, archivo contenedor de correos electrónicos, disco duro, etc. Se realizará mediante copia y depósito de la información ante notario<sup>73</sup>. En el caso de que una inexistente o deficiente cadena de custodia no implica automáticamente la nulidad de la prueba, pero sí que es real que puede afectar a su fiabilidad.

En la STS 587/2014, de 18 de julio<sup>74</sup>, se define la cadena de custodia como un sistema formal de garantías destinado a asegurar que la prueba no haya sido alterada. En este sentido, en la STS 287/2017, de 19 de abril, el Tribunal Supremo<sup>75</sup> advierte que *“la ruptura de la cadena de custodia no supone el expreso reconocimiento de dudas acerca de la integridad de la prueba, sino que se tendrá que aportar de forma objetiva un razonamiento del motivo de la ruptura”*<sup>76</sup>.

---

<sup>71</sup> Pérez Asenjo, A. I., “Registro físico y remoto de dispositivos de almacenamiento masivo y sistemas informáticos”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 59, p. 39.

<sup>72</sup> Ibid., pp. 15–16.

<sup>73</sup> Pasamar, A., “La prueba pericial informática frente a la impugnación de la autenticidad de un e-mail”, 2011 (disponible en <http://www.esade.edu/itemsweb/content/produccion/4010660.pdf>); Última consulta 26 de febrero de 2026.

<sup>74</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 587/2014, de 18 de julio (versión electrónica-base de datos VLEX) Fecha de última consulta: 10 de febrero de 2026.

<sup>75</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 287/2017, de 19 de abril (versión electrónica-base de datos VLEX). Fecha de última consulta: 10 de febrero de 2026.

<sup>76</sup> Pérez Asenjo, A. I., “Registro físico y remoto...”, op. cit., p. 39. op. cit., p. 17.

## CAPÍTULO IV. LAS REDES SOCIALES COMO FUENTES DE PRUEBA

### 1. LAS REDES SOCIALES COMO FUENTE DE PRUEBA ELECTRÓNICA EN EL PROCESO JUDICIAL

La forma en que la sociedad se relaciona ha sufrido una transformación con la aparición de las redes sociales, convirtiéndose éstas en un espacio virtual de comunicación habitual entre los usuarios y desde un punto de vista jurídico en una fuente constante de información relevante.

La aparición de la prueba tecnológica ha supuesto un reto para la jurisprudencia y la doctrina ya que se ha tenido que evolucionar hacia la admisión y la incorporación en la ley de los medios de prueba digitales como lo son las publicaciones, mensajes privados, comentarios o vídeos difundidos a través de las redes sociales siempre bajo determinados requisitos jurisprudenciales y desarrollados por el TS en cuanto a su obtención, autenticidad, integridad y valor probatorio.

Según el Instituto Nacional de Tecnologías de la Comunicación, las redes sociales se definen como *“aquellos servicios que se prestan a través de internet y que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de los usuarios afines o no al perfil publicado”*. Pueden tener una utilización o finalidad limitada al ocio o por el contrario tener un uso profesional.<sup>77</sup>

#### **1.1 Requisitos jurisprudenciales para la validez de la prueba tecnológica procedente de redes sociales**

La inclusión en los procesos legales de pruebas procedentes de redes sociales ha sido objeto de un notable desarrollo en la jurisprudencia debido a la falta de una regulación específica, por ello, los juzgados y en especial el TS han establecido unos criterios que deben ser cumplidos para que la prueba que se pretende aportar al proceso sea aceptada y evaluada de manera válida.

---

<sup>77</sup> López Hormeño, M. del C., “Las fuentes de obtención de la prueba tecnológica: los correos electrónicos, el WhatsApp y las redes sociales”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 32, 2022, pp. 9-13.

### 1.1.1 Autenticidad del contenido

La facilidad de alteración de las evidencias procedentes de redes sociales es tan alta que por eso llevó al Tribunal Supremo a enumerar este primer criterio jurisprudencial para que tal prueba sea considerada válida. Así, capturas de pantalla, mensajes (en cuanto a la hora y fecha de envío e incluso su contenido) o publicaciones pueden ser modificados, descontextualizados o incluso fabricados desde cero, o como jurídicamente también se podría decir, creados ex novo<sup>78</sup>.

Por esta razón, la doctrina requiere demostrar de manera suficiente que la prueba presentada reúna todas estas características: la autenticidad, falta de manipulabilidad y no alterabilidad, que sea correspondiente a una publicación real efectuada en la red social de la que se proceda<sup>79</sup>.

El TS destaca la importancia de la autenticidad, en su Sentencia número 300/2015 de 19 de mayo<sup>80</sup> en la que declaró en relación a los mensajes y contenidos obtenidos de redes sociales que *“no pueden ser considerados dichos mensajes por sí solos como prueba suficiente cuando la autenticidad de los mismos sea impugnada”*.

### 1.1.2 Identificación del titular de la cuenta

Otro de los requisitos es la capacidad de demostrar una vinculación real del contenido de la prueba a una persona determinada. No basta con acreditar que dicha publicación, imagen o vídeo existe, sino que, además, tiene que verificarse que el perfil de la red social desde la que se publica realmente le pertenece a la persona que se menciona y que el autor concreto tenía un control efectivo sobre la misma en el momento de la publicación<sup>81</sup>.

Resulta esencial para descartar pruebas digitales que tengan su origen en cuentas fraudulentas o falsas, suplantadas o utilizadas por personas distintas del titular sin consentimiento de éste. Así se ratifica por la STS 754/2015, de 27 de noviembre, que estableció que la titularidad

---

<sup>78</sup> Rubio Alamillo, J., “Adquisición y presentación en un procedimiento judicial de una prueba informática”, El Derecho, 4 de abril de 2017 (disponible en [https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica?utm\\_source=](https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica?utm_source=); última consulta 18/03/2026).

<sup>79</sup> Mas Carrillo, M., “Proceso laboral: prueba digital y protección de datos. Aspectos procesales”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 13, Madrid, 2020, pp. 36-37.

<sup>80</sup> Tribunal Supremo, STS 300/2015, op. cit.

<sup>81</sup> Lloria García, P., “Infancia, adolescencia y nuevas tecnologías según la Ley Orgánica 8/2021”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 17, Madrid, 2022, pp.5-7

formal de una cuenta no prueba automáticamente la autoría de los mensajes por los motivos expuestos de suplantación o anonimato.

### **1.1.3 Integridad y preservación de la evidencia**

La integridad hace referencia a que el contenido de la prueba tecnológica se mantenga original y no haya sufrido ninguna alteración desde su obtención, es decir, que el contenido presentado en el proceso coincida completamente con el original<sup>82</sup>. El requisito de integridad demuestra la veracidad del contenido de la prueba al Tribunal cuando se conserva en su formato original (mediante la presentación del teléfono móvil en el proceso, por ejemplo), y existe cadena de custodia.

También es posible la implementación o utilización de mecanismos que demuestren la inalterabilidad del contenido. La importancia de la preservación de la evidencia y su integridad queda plasma en la STS 489/2018, de 23 de octubre<sup>83</sup>, que exige la acreditación de que la prueba se ha mantenido inalterada desde el momento de su creación hasta su efectiva aportación al proceso señalando que las capturas de pantalla resultan insuficientes necesitando de pruebas complementarias para demostrar su veracidad a través de pruebas periciales<sup>84</sup>.

### **1.1.4 Posibilidad de contradicción/impugnación**

Las pruebas tecnológicas, al igual que los medios de prueba convencionales, deben respetar el principio de contradicción, garantizando a la parte contraria la posibilidad de impugnar la prueba cuando existan dudas fundadas y constatadas acerca de su autenticidad o su autoría. La contraparte también estará autorizada para solicitar pruebas adicionales como lo es la pericial informática<sup>85</sup>. Este derecho queda recogido en la STS 754/2015<sup>86</sup> que insiste en que la valoración de la prueba por el Tribunal tiene que garantizar en todos los casos la posibilidad de contradicción por la contraparte.

---

<sup>82</sup> Rubio Alamillo, J., *op. cit.* (disponible en [https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica?utm\\_source](https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica?utm_source); última consulta 18/03/2026).

<sup>83</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 489/2018, de 23 de octubre (recurso de casación núm. 1674/2017) (versión electrónica-base de datos VLEX). Fecha de última consulta: 1 de febrero de 2026

<sup>84</sup> Rivas Velasco, M. J., “Documento electrónico...”, *op. cit.*, pp. 3–7.

<sup>85</sup> Pérez Asenjo, A. I., “Registro físico y remoto...”, *op. cit.*, p. 29.

<sup>86</sup> Tribunal Supremo, STS 754/2015, *op. cit.*

### **1.1.5 Confirmación de la veracidad de la prueba tecnológica a través de la pericial informática**

En caso de impugnación de la prueba, la jurisprudencia suele exigir la aportación al proceso de una prueba pericial informática, realizada por un perito profesional en su campo, que permita verificar la autenticidad del contenido, acreditar su origen y verificar de forma exacta otros aspectos como la fecha, la hora y los metadatos concretos de la prueba<sup>87</sup>, así lo establece la STS 300/2015 de 19 de mayo.

### **1.1.6 Respeto a los derechos fundamentales**

Por último, la obtención de la prueba digital se debe realizar respetando los derechos fundamentales, ya que, en caso de colisión con el derecho a la intimidad, el secreto de las telecomunicaciones, la prueba deviene ilícita y se debe inadmitir por el Tribunal<sup>88</sup>. La STS 114/2017<sup>89</sup> rechaza la posibilidad de valoración de una prueba obtenida ilícitamente con vulneración de los derechos fundamentales o libertades públicas<sup>90</sup>.

La jurisprudencia ha configurado un sistema riguroso, exigiendo unos requisitos de autenticidad, autoría, integridad, contradicción y licitud en su obtención. Por consiguiente, una publicación en redes sociales constituye una fuente de prueba, pero sólo se convierte en evidencia judicial si supera el examen de los requisitos mencionados.

## **2. VALIDEZ Y EFICACIA PROBATORIA DE LAS PRUEBAS DIGITALES PROCEDENTES DE “WHATSAPP”.**

En lo que respecta a la naturaleza de los mensajes de mensajería móvil instantánea, existe un gran debate en la doctrina acerca de si deben encajarse dentro del concepto amplio de documento electrónico o por el contrario, ser considerados como una fuente de prueba electrónica autónoma cuya eficacia probatoria depende de su posterior autenticación mediante otros medios complementarios<sup>91</sup>.

---

<sup>87</sup> Suárez Robledano, J. M., “La relevancia de la prueba electrónica en la lucha contra los delitos informáticos”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 52, Madrid, 2009, pp. 9-11.

<sup>88</sup> López Hormeño, M. del C., “Las fuentes de obtención...”, *op. cit.*, pp. 10-14.

<sup>89</sup> Sentencia del Tribunal Supremo, Sala Quinta, núm. 114/2017, de 21 de noviembre (versión electrónica-base de datos VLEX). Fecha de última consulta: 1 de marzo de 2026.

<sup>90</sup> Rivas Velasco, M. J., “Documento electrónico...”, *op. cit.*, pp. 10-12.

<sup>91</sup> Taléns Visconti, E. E., “La revisión de hechos probados en el recurso de suplicación: la naturaleza jurídica de la prueba basada en una conversación de WhatsApp”, *Revista Española de Derecho del Trabajo*, n.º. 231, 2020.

Una de las primeras tesis sostuvo que el soporte a papel que transcribe una conversación de WhatsApp no puede considerarse prueba documental sino una prueba electrónica constituyente de una mera transcripción del contenido de una prueba electrónica del artículo 299.2 LEC <sup>92</sup>. Las sentencias del TSJ de Cantabria de 11 de diciembre de 2015 <sup>93</sup> y del TSJ de Islas Canarias, de 16 de abril de 2018 <sup>94</sup> apoyan esta postura. La postura contraria sostuvo al respecto que dada su parecido con el correo electrónico impreso (contando este con naturaleza de documento privado) las conversaciones de mensajería instantánea deben recibir el mismo tratamiento jurídico. Por ello, su valor probatorio dependerá de si son reconocidas por la parte contraria o impugnadas quedando entonces a la libre valoración por el tribunal conforme a las reglas de la sana crítica. En concreto, El TSJ de Asturias de 26 de diciembre de 2019<sup>95</sup> no rechaza el carácter documental estas pruebas, asimilando su carácter documental al correo electrónico, pero sí su eficacia a la hora de probar un hecho.

El TS ha admitido que la aportación de conversaciones de WhatsApp en un proceso judicial pueda constituir una prueba documental auténtica, siempre que se encuentre sujeta a determinados requisitos como la obtención lícita de los mensajes y su autenticidad. Así lo establece la Sentencia núm. 300/2015 de la Sala 2ª de lo Penal del Tribunal Supremo <sup>96</sup> en la que se destaca la importancia de tratar con cuidado la prueba de comunicaciones bidireccionales por mensajería instantánea, ya que pueden ser manipuladas, permitir el anonimato o la creación de identidades falsas. La sentencia señala que la carga de la prueba corresponde a quien se beneficia de su valor probatorio y subraya que, si se cuestiona la autenticidad, es necesaria una prueba pericial <sup>97</sup>. En línea con lo anterior, la STS nº1066/2009 de 4 de noviembre, también establece que la prueba contenida en soportes telemáticos u obtenida a través de ellos gozará de validez y eficacia de un documento original, previamente cumplidos los requisitos de autenticidad e integridad<sup>98</sup>.

---

<sup>92</sup> Ibid.

<sup>93</sup> Sentencia del Tribunal Superior de Justicia de Cantabria, de 11 de diciembre de 2017 (recurso núm. 859/2015) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 18 de marzo de 2026

<sup>94</sup> Sentencia del Tribunal Superior de Justicia de Islas Canarias, de 16 de abril de 2018 (recurso núm. 799/2017) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 1 de febrero de 2026.

<sup>95</sup> Sentencia del Tribunal Superior de Justicia de Asturias, de 26 de diciembre de 2019 (recurso núm. 2232/2019) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 10 de marzo de 2026.

<sup>96</sup> Tribunal Supremo, STS 300/2015, op. cit.

<sup>97</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, op. cit., pp. 260-270,

<sup>98</sup> Beltrán Pardo, A. I., “Los contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo”, Noticias Jurídicas, 30 de septiembre de 2015

Por otro lado, el artículo 3.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (derogada por la Ley 6/2020) que recoge la definición de documento electrónico, siendo este aquel que tenga naturaleza electrónica y esté archivado en un soporte electrónico siguiendo un formato determinado y susceptible de identificación y tratamiento diferenciado.

Por tanto, un documento electrónico también puede ser el soporte de un documento privado, encajando en esta clasificación el “WhatsApp” pues no deja de ser un contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual vinculado a un número de teléfono<sup>99</sup>. Si una parte presenta como medio de prueba un WhatsApp está legitimada para adoptar los dictámenes y medios de prueba instrumentales que considere pertinentes, así como presentarlas si la contraparte cuestione la autenticidad de lo reproducido. La validez de la prueba puede ser cuestionada por cualquiera de las dos partes o incluso del Tribunal en el momento de la proposición de la prueba.

Las pruebas procedentes de aplicaciones de mensajería instantánea pueden aportarse en soporte papel (pantallazos impresos de conversaciones o transcripciones de mensajes) o mediante la terminal o móvil, es decir, la presentación al Tribunal del teléfono que permite comprobar de forma directa las conversaciones que sirven de prueba, o practicar una pericial informática<sup>100</sup>.

Constituye un medio de prueba complejo y por ello se necesitan otros medios de prueba para demostrar su autenticidad y su alcance. Si bien es cierto que un WhatsApp es fácilmente manipulable, también son susceptibles de sufrir esta manipulación los testigos e incluso los peritos y por ello los tribunales deben valorar cada prueba conforme a las reglas de su sana crítica (art. 382 LEC). En lo que respecta a la cadena custodia, el Notario y el Letrado de la Administración de Justicia pueden reflejar en el acta correspondiente la fecha y hora exacta del respectivo mensaje además del contenido literal tal y como se reflejan en el teléfono móvil, pero hasta ahí llega su valor probatorio, necesitando de un medio de prueba instrumental<sup>101</sup>.

---

(disponible en <https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533-las-contenidos-de-whatsapp-como-medio-probatorio-en-el-ambito-de-las-diligencias-urgente/>; última consulta 10/03/2026).

<sup>99</sup> López Hormeño, M. del C., “Las fuentes de obtención...”, *op. cit.*, p. 9.

<sup>100</sup> *Ibid.*, p. 12.

<sup>101</sup> Abel Lluch, F. J., “El documento electrónico...”, *op. cit.*, pp. 6–8.

La STSJ de Galicia 556/2016, de fecha de 27 de enero <sup>102</sup>afirma en relación con los medios probatorios cuyo origen es el WhatsApp que no sólo constituye un medio de prueba válido pese a no contemplarse en la LJS sino que ya ha tenido plasmación normativa. Se establecen una serie de requisitos que debían cumplirse para que la conversación de WhatsApp tenga la consideración de documento a efectos del proceso; debe aportarse no sólo la copia de la impresión de pantalla, es decir, el “Pantallazo” sino también una transcripción de la conversación y la verificación de que coincide efectivamente con el número de teléfono relacionado<sup>103</sup>.

Una conversación de esta aplicación de mensajería instantánea será admisible en el proceso como documento siempre que estemos dentro de estos cuatro supuestos:

1. Que la contraparte no impugne la conversación o mensaje, es decir, que no haya discusión ninguna acerca de la autenticidad e integridad de esta<sup>104</sup>.
2. Que haya un reconocimiento expreso de la mencionada conversación y, por ende, de su contenido; Se trata de un reconocimiento explícito de la otra parte acerca de la existencia de la conversación.
3. Cuando se compruebe su autenticidad mediante el cotejo con otro el otro terminal implicado, en otras palabras, se contraste el mensaje con el teléfono de la otra parte a través de la exhibición judicial.
4. En el caso de que no se cumplan ninguna de las anteriores situaciones es determinante la prueba pericial informática, supuesto que en la práctica ocurre ante la impugnación de la autenticidad del WhatsApp.

Siguiendo lo anterior, debido a su fácil manipulación, el Juez debe examinar en cada uno de los casos dichas pruebas y rechazar su eficacia probatoria si existen dudas fundadas acerca de su autenticidad. Por el contrario, si ambas partes reconocen el contenido del WhatsApp, la conversación pasa a formar parte del proceso, y de esta forma, del conjunto de pruebas válidamente practicadas<sup>105</sup>.

---

<sup>102</sup> Sentencia del Tribunal Superior de Justicia de Galicia, de 27 de enero de 2016 (recurso núm. 556/2016) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 7 de marzo de 2026.

<sup>103</sup> Tardón Olmos, M., “La violencia de género...”, op. cit., pp.17-20

<sup>104</sup> Beltrán Pardo, A. I., *op. cit.* (disponible en <https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533-las-contenidos-de-whatsapp-como-medio-probatorio-en-el-ambito-de-las-diligencias-urgente/>; última consulta 10/03/2026)

La STS número 300/2015 de 19 de mayo<sup>106</sup> resulta clave en este aspecto al considerar que estas pruebas son aptas para incorporarse al proceso siempre que se acredite su autenticidad, inalterabilidad, no manipulación e integridad. Dicha doctrina ha sido reiterada en múltiples sentencias posteriores como la STS 754/2015 de 26 de noviembre<sup>107</sup> que vuelve a recalcar que la pericial informática no opera automáticamente ante una impugnación en el caso de que el Tribunal tenga un conocimiento y convicción fundado acerca del origen y de la fiabilidad de la prueba digital.

En relación con las redes sociales y aplicaciones de mensajería instantánea, el TS en la sentencia 119/2019<sup>108</sup> subraya que este tipo de prueba tiene que ser valorada de forma conjunta con el resto de material probatorio, teniendo relevancia el acceso al soporte original y la existencia de corroboraciones externas. Relacionado con este último punto, la STS 375/2018 de 19 de julio<sup>109</sup> considera este tipo de pruebas válidas siempre que se cumplan determinadas condiciones; necesidad de aportación junto a la prueba del soporte original, cumplimiento del principio de contradicción y la ausencia de indicios de cualquier tipo de manipulación.

### 3. EL CORREO ELECTRÓNICO COMO MEDIO DE PRUEBA EN EL PROCESO CIVIL

El correo electrónico constituye un sistema instantáneo de comunicación de textos, imágenes y sonidos entre uno o múltiples destinatarios, mediante el uso de unas direcciones electrónicas previamente conocidas por ambos<sup>110</sup>. En cuanto a su naturaleza probatoria, se reconoce que el correo electrónico tiene naturaleza de prueba documental, incluso cuando su aportación al proceso se hace en soporte papel.<sup>111</sup> Así lo establece la STS 706/2020 de 23 de julio<sup>112</sup> al afirmar que no se puede excluir la naturaleza documental del correo electrónico.

La naturaleza documental queda amparada inicialmente bajo la Ley 59/2003 de Firma Electrónica posteriormente derogada por la Ley 6/2020, de 11 de noviembre, reguladora de

---

<sup>106</sup> Tribunal Supremo, STS 300/2015, op. cit.

<sup>107</sup> Tribunal Supremo, STS 754/2015, op. cit.

<sup>108</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 119/2019, de 6 de marzo (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 12 de marzo de 2026.

<sup>109</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 375/2018, de 19 de julio versión electrónica-base de datos CENDOJ). Fecha de última consulta: 12 de marzo de 2026.

<sup>110</sup> Ortuño Navalón, M.<sup>a</sup> del Carmen, “La prueba electrónica...”, op. cit.

<sup>111</sup> Consejo General del Poder Judicial, “Nuevas tecnologías, prueba y protección de datos: conclusiones”, *Cuadernos Digitales de Formación*, n.º 72, Madrid, 2021, pp. 5–8.

<sup>112</sup> Sentencia del Tribunal Supremo, Sala Segunda, núm. 706/2020, de 23 de julio (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 1 de febrero de 2026.

determinados aspectos de los servicios electrónicos de confianza, que complementan el marco legal creado por el Reglamento (UE) núm. 910/2010 (eIDAS). Asimismo, se determina en los artículos 299 y 333 de la LEC siempre que sea susceptible de identificación, archivo y reproducción de la prueba documental y pueda aportarse al proceso en soporte papel o mediante documento electrónico.

El término en soporte papel hace referencia a la impresión del correo concreto, recibiendo el tratamiento de documento privado. Sin embargo, este puede impugnado fácilmente si no se acompaña de los documentos necesarios que acrediten su autenticidad como una certificación o informe pericial. Además, presentar el documento electrónico, es decir, el archivo digital en un CD, USB u otro medio donde se encuentre la prueba refuerza la credibilidad frente a su presentación exclusiva en soporte papel<sup>113</sup>.

En consonancia con la firma electrónica, esta es especialmente importante pues sin ella, el correo electrónico es técnicamente manipulable<sup>114</sup>, y así queda establecido en la SAP Cádiz, Sección 2.ª, 79/2008 de 25 de febrero, que aborda el valor probatorio dado a unos documentos *“constituidos por copias privadas obtenidas de documentos electrónicos (e-mails o correos electrónicos) que no consta que posean firma electrónica reconocida y que han sido obtenidos a través de la impresora de un ordenador”* y que habían sido impugnados por la contraparte en cuanto a su autenticidad como a su contenido, concluyendo que si no hay prueba alguna que acredite el envío y el contenido no podrá admitirse.

Un correo electrónico normal puede ser impugnado, pero no el correo certificado pues es casi imposible de alterar, debido a que las compañías de certificación electrónica recogen todo tipo de pruebas de la comunicación, actuando como un tercero imparcial y encargándose de que las actas de comunicación que prueban la transmisión quedan guardadas ante notario. Todas estas certificaciones quedan legitimadas por el Auto del TS 2501/2013<sup>115</sup> en donde acreditó que dicha forma de comunicación a través de la certificación cumple plenamente con las exigencias legales del artículo 162 LEC que permite la realización de actos de comunicación por medios

---

<sup>113</sup> Velasco Núñez, E., “Correo electrónico, SMS y “virus troyanos”: aspectos procesales penales”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 22, Madrid, 2009, p. 26-27.

<sup>114</sup> Rubio Alamillo, J., “El correo electrónico como prueba en procedimientos judiciales”, *Diario La Ley*, n.º 8808, 21 de julio de 2016, Editorial Wolters Kluwer, p. 7 (disponible en <https://peritoinformaticocolegiado.es/wp-content/uploads/El-correo-electronico-como-prueba-en-procedimient....pdf>; última consulta 23/03/2026).

<sup>115</sup> Auto del Tribunal Supremo, Sala Segunda, núm. 2501/2013 (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 13 de marzo de 2026.

electrónicos siempre que quede garantizado el contenido de la comunicación, su autenticidad y la constancia de su recepción<sup>116</sup>.

Los correos electrónicos también se pueden impugnar en lo que respecta a su autenticidad y contenido. Si la prueba se presenta en papel y la otra parte no cuestiona su autenticidad, al igual que en el WhatsApp, suele aceptarse. En estos casos, los correos deben presentarse en formato digital para que así los peritos puedan analizarlos ya que una simple copia en papel no garantiza su autenticidad. Desde un punto de vista técnico, es imposible aportar el correo original recibido puesto que los servidores no guardan los mensajes una vez enviados al destinatario. Por eso, a la hora de examinar su autenticidad, será necesario la clonación del disco duro del servidor ante notario<sup>117</sup>.

El problema que plantea la pericial en el campo del correo electrónico es la dificultad de que la cadena de custodia ha de ser averada fehacientemente para poder acceder a las fuentes de información y poder emitir un dictamen sobre si ha habido o no manipulación, tal como indica PASAMAR<sup>118</sup>. El mail es una prueba válida, pero mientras el correo electrónico ordinario es una *fotocopia* que requiere autenticarse, el correo electrónico certificado es un *acta* que ofrece certeza.

#### 4. LA POSIBLE VULNERACIÓN DE DERECHOS FUNDAMENTALES Y LA REGLA DE EXCLUSIÓN.

La incorporación de la prueba digital puede cruzar en determinados casos el límite de los derechos fundamentales del artículo 18 de la CE cuando se trata de la aportación del correo electrónico al proceso.

En la STC núm. 114/1984 se define el contenido del secreto a las comunicaciones como un derecho de carácter formal, extendiéndose la protección constitucional tanto al contenido del

---

<sup>116</sup> Espada Bueno, P., “El correo electrónico como prueba judicial: ¿Tiene validez?”, El Derecho, 6 de junio de 2018 (disponible en <https://elderecho.com/el-correo-electronico-como-prueba-judicial-tiene-validez>; última consulta 10/03/2026).

<sup>117</sup> Rubio Alamillo, J., “El correo electrónico...”, op. cit., pp. 3-5.

<sup>118</sup> Pasamar, A., op. cit. (disponible en <http://www.esade.edu/itemsweb/content/produccion/4010660.pdf>; última consulta 26 de febrero de 2026),

mensaje como a todo lo que se une a él accesoriamen<sup>119</sup>. La STC 4/1996<sup>120</sup> reafirma que la comunicación es constitucionalmente impenetrable para terceros ajenos a ella, afirmación que se extiende en lo que sea aplicable para el correo electrónico y a las comunicaciones en redes sociales. Ante posible invasión de terceros distintos de las involucradas en la conversación, la ley prevé la necesidad de autorización judicial ante la grabación de las comunicaciones, debido al carácter secreto erga omnes de las comunicaciones <sup>121</sup>. Esta doctrina ha sido reiterada SSTC 59/2003, 241/2012 y 170/2013 que resaltan la importancia de la necesidad de preservar la privacidad frente a injerencias no legitimadas, incluso hablando de entornos tecnológicos<sup>122</sup>.

La regla de exclusión opera en aquellos supuestos en los que la obtención de correos electrónicos o mensajes cuyo origen son las redes sociales se produce mediante el acceso no autorizado a cuentas ajenas o perfiles protegidos por contraseñas. En estos supuestos, se está produciendo una vulneración del derecho al secreto de las telecomunicaciones, determinando automáticamente la ineficacia probatoria de la evidencia, de acuerdo con lo establecido en el artículo 11.1 de la Ley Orgánica del Poder Judicial<sup>123</sup>. Esta regla no opera en los casos en los que la prueba es aportada por el propio receptor de la comunicación puesto que dispone legítimamente del contenido y su obtención no tiene un origen ilícito.

Un ejemplo ilustrativo de una conversación extraída de una aplicación de mensajería instantánea admitida como prueba lícita es la SAP número 702/2015 de 24 de noviembre<sup>124</sup> en la que se aportaron mensajes de WhatsApp como medio probatorio. La parte recurrente alegó que dicha conversación infringía el derecho al secreto de las telecomunicaciones, pero el Tribunal lo negó al haber sido aportadas las conversaciones por la parte destinataria de la comunicación estando legitimada a hacerlo. La conclusión fue que el alcance del mencionado derecho fundamental únicamente se restringe para terceros ajenos a la conversación, no a los interlocutores de esta.<sup>125</sup> En consecuencia, no puede hablarse en ningún momento de interceptación ilícita, vulneración del artículo 18 CE y la naturaleza no probatoria de la prueba.

---

<sup>119</sup> Orellana Cano, N. A., “La prueba en el tráfico mercantil...”, op. cit., pp. 36-37.

<sup>120</sup> Sentencia del Tribunal Constitucional, núm. 34/1996, de 11 de marzo (versión electrónica-base de datos del Tribunal Constitucional). Fecha de última consulta: 1 de febrero de 2026.

<sup>121</sup> García Pérez, M. F., “Nuevas tecnologías y derechos humanos...”, op. cit., pp. 9, 14.

<sup>122</sup> López Hormeño, M. del C., “Las fuentes de obtención...”, op. cit., pp. 12-13.

<sup>123</sup> Muñoz Aranguren, A., “El tratamiento de la prueba ilícita por la reciente jurisprudencia de la Sala Segunda del TS: algunas tendencias”, Revista Aranzadi de Derecho y Proceso Penal, n.º 77, 2025.

<sup>124</sup> Sentencia de la Audiencia Provincial, núm. 702/2015, de 24 de noviembre (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 19 de marzo de 2026

## 5. PROTECCIÓN DE DATOS Y VALORACIÓN PROCESAL

El uso de redes sociales ha conllevado que publicaciones, comentarios, mensajes privados y compartidos a través de aplicaciones como Instagram, Facebook, Twitter etc. se hayan convertido en fuentes de prueba en los procesos judiciales. No obstante, su empleo suscita relevantes dudas desde el punto de vista de los derechos fundamentales y garantías procesales, requiriendo un examen para determinar los límites de su utilización como fuentes de prueba y hasta qué punto pueden incorporarse al proceso judicial.

El TC ha interpretado el artículo 18.4 CE para establecer el derecho fundamental a la protección de datos personales. El mismo recoge que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” constituyendo una cláusula abierta y general. Dado a su carácter de cláusula abierta, sólo pueden ser actividades inconstitucionales las leyes que se aparten del marco constitucional, quedando reflejado este planteamiento en la STC 254/1993 que reconoció por primera vez un derecho fundamental a la protección de datos distinto del derecho a la intimidad<sup>126</sup>.

A nivel europeo, este derecho está reconocido en el artículo 8 CEDH<sup>127</sup> “Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan”, impidiendo de esta manera su monitorización indiscriminada sin base legal suficiente. Por lo que, en cuanto a la vulneración de los derechos fundamentales, a las redes sociales le es aplicable la misma doctrina establecida para los correos electrónicos, basándose en la protección de la esfera de la privacidad y la protección extendida de los accesorios de la comunicación.

La obtención de cualquier mensaje, foto, vídeo procedente de una red social que se haya realizado sin consentimiento o incluso desconocimiento del afectado determinará la ilicitud de la prueba y su consiguiente expulsión y exclusión del proceso según lo establecido en el artículo 11.1 de la Ley Orgánica del Poder Judicial.

---

<sup>126</sup> Troncoso Reigada, A., “La protección de datos personales. En busca del equilibrio”, Tirant lo Blanch, Valencia, 2010, p. 110-115.

<sup>127</sup> Artículo 8 del Convenio Europeo de Derechos Humanos

Resulta relevante la STS núm.82/2018, de 15 de octubre<sup>128</sup>, donde se establecieron los criterios que deben seguir la valoración de pruebas procedentes de las redes sociales. El caso se refiere a mensajes y fotografías difundidas por Facebook y WhatsApp, pero la doctrina establecida se puede trasladar al resto de redes sociales, como Instagram, que comparte la misma naturaleza técnica que las dos anteriores junto a su facilidad de manipulación.

El TS insiste en que la red no es suficiente por sí misma, para establecer quién fue el creador ni su verdadero origen, debido a la capacidad técnica de modificar, duplicar y generar perfiles falsos o anónimos. Consolida así la determinación de que la prueba pericial en los casos en los que se aportan ante el Tribunal contenidos procedentes de redes sociales no es meramente un elemento accesorio sino un elemento indispensable, para examinar los metadatos asociados al archivo y acreditar la no manipulabilidad, integridad y autenticidad de la prueba.

Por otro lado, la LOPD<sup>129</sup> exige que cualquier tratamiento de datos personales, incluido el realizado por redes sociales, cuente con los siguientes requisitos; consentimiento expreso e informado del usuario, obligación de información acerca del uso, cesión y transferencia interna de dichos datos, así como a establecer mecanismos para que los usuarios puedan ejercer sus derechos. Por último, esta ley impone condiciones restrictivas a la comunicación de datos personales a terceros, incluyendo empresas, con el fin de garantizar la transparencia y responsabilidad de las redes sociales.

En cuanto a la inversión de la carga de la prueba procedente de redes sociales, ¿dicha carga deberá exigirse a quien impugna la autenticidad y la consiguiente manipulación o por el contrario deberá recaer sobre quien defiende su integridad desde un primer momento? La jurisprudencia y doctrina han aceptado de forma mayoritaria que la carga de la prueba la ostente quien cuestiona la veracidad de la prueba digital, pero esto claramente plantea problemas en estos casos de pruebas digitales cuyo origen radica en las redes sociales, dada su fácil alteración y suplantación<sup>130</sup>.

---

<sup>128</sup> Sentencia del Tribunal Supremo (Sala Quinta, de lo Militar), núm. 82/2018, de 15 de octubre) (versión electrónica-base de datos vLex). Fecha de última consulta: 2 de marzo de 2026.

<sup>129</sup> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018).

<sup>130</sup> Troncoso Reigada, A., “La protección de datos personales...”, op. cit., pp. 120-122

Por consiguiente, si se continuase exigiendo a la parte impugnante la demostración de tal manipulación, esto haría que recayese sobre dicha parte una carga técnica desproporcionada, generando con ello una asimetría probatoria contraria a la igualdad de armas y por ende, un daño al derecho de defensa.

## **CAPÍTULO V. IMPUGNACIÓN DEL DOCUMENTO ELECTRÓNICO Y PRUEBA PERICIAL**

### **1. CONCEPTO DE IMPUGNACIÓN DE LA PRUEBA EN EL PROCESO CIVIL**

Para entender el complejo concepto de impugnación del documento electrónico, es necesario remitirse al artículo 427.1 de la LEC que establece *“En la audiencia previa, cada parte se pronunciará sobre los documentos aportados de contrario hasta ese momento, manifestando si los admite, impugna o reconoce o si, en su caso, propone prueba acerca de su autenticidad”*.

A la hora de comprender el triple posicionamiento que se deriva del mencionado artículo (reconocimiento, admisión o impugnación), hay que analizar previamente la SAP de Lleida 411/2022<sup>131</sup>, de la que se puede extraer la siguiente jurisprudencia.

La Sentencia establece que, conforme al artículo 427.1 LEC, la finalidad de la impugnación de la contraparte en la audiencia se limita exclusivamente a cuestionar la autenticidad formal. Ello implica que la impugnación del documento debe fundamentarse en la falsedad, manipulación o dudas respecto a su origen y no por objeciones relativas a su contenido o valor probatorio ya que se excedería de la línea de la autenticidad formal. En el caso de que una parte guarde silencio se entiende automáticamente que no pone ninguna objeción al documento, y en el caso de que lo impugne deberán razonadamente explicitarse los motivos de la impugnación<sup>132</sup>.

Esto, trasladado a la práctica, supone que, en un procedimiento civil ordinario, cuando la parte demandante aporte, en la audiencia previa un documento electrónico, una captura de pantalla de una conversación de WhatsApp, la demandada no puede impugnar el documento alegando que no está de acuerdo con el contenido del mensaje y negando el valor probatorio de la conversación.

---

<sup>131</sup> Sentencia de la Audiencia Provincial de Lleida, Sección 2.ª, núm. 411/2022, de 17 de junio (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 9 de marzo de 2026.

<sup>132</sup> Abel Lluch, F. J., “El documento electrónico...”, *op. cit.*, pp. 12–16.

Dicha impugnación no resulta válida porque no se discute la autenticidad formal. En el caso de discutir la falta de autenticidad de la prueba, se estaría aludiendo a la falta de coincidencia entre el autor aparente y el real, es decir, que el documento no ha sido redactado por el autor inicial que alega la parte. La falta de integridad alude a la posibilidad de que el documento ha sido modificado mediante la sustitución, incorporación o la eliminación de palabras. Lo que no constituye motivo válido de impugnación en la audiencia previa es hacer referencia alguna a la falta de veracidad del documento, a su ilicitud derivada de la infracción de derechos fundamentales en su obtención y a la posible extemporaneidad en la presentación de la prueba<sup>133</sup>.

La finalidad del posicionamiento no es otra que acreditar por la contraparte la autenticación del documento, configurándose de esta forma como una carga procesal. Por tanto, la parte tendrá tres opciones:

1. Reconocer el documento suscrito por la parte
2. Admitir que la parte, aunque no haya suscrito el documento lo reconoce como auténtico y no lo manipula
3. Impugnar el documento porque tiene dudas fundadas acerca de la autenticidad formal del mismo o del testimonio. Es decir, que alega que no es auténtico.

En vista de lo anterior, se pueden distinguir los siguientes escenarios: Si se impugna la falta de autenticidad, integridad, precisión de fecha u otra característica sin intervención de persona física o jurídica cuya finalidad es garantizar la autenticidad e integridad de los documentos electrónicos, se debe valorar en sentencia conforme al criterio de la regla de la sana crítica, atendiendo en su caso a la prueba pericial. En caso contrario, si interviene un prestador de confianza cualificado, se presume que el documento impugnado es auténtico, íntegro y preciso en la fecha y la carga de efectuar la comprobación corresponde a quien haya presentado la impugnación en base al Art. 326 LEC<sup>134</sup>.

La posibilidad de impugnar el documento alegando dudas fundadas con respecto a la certeza, veracidad y fuerza probatoria del mismo, podrá tener lugar en un momento distinto al de la audiencia previa. Se permiten dichas impugnaciones en momentos procesales como durante el

---

<sup>133</sup> Ibid., pp. 12-16.

<sup>134</sup> Ibid., p. 17.

acto del juicio y en el trámite de conclusiones. El Art. 326.2 LEC establece que se deberá valorarse en sentencia el documento impugnado junto a los demás medios de prueba, atendiendo a las reglas de la sana crítica.

## 6. OBJETO Y FINALIDAD. REQUISITOS DEL INFORME

De los arts. 335.1 y 352 se puede inferir el carácter especial de la prueba pericial, distinto al de los demás medios de prueba. Esto se debe a la necesidad de que el conocimiento que aporte el perito a través de su dictamen sea fundamental, universal y esté desligado del caso concreto que se enjuicia en el proceso<sup>135</sup>.

La función del perito radica en aportar al proceso, mediante un dictamen pericial, conocimientos técnicos, científicos, artísticos o prácticos a fin de que el juez pueda apreciar los hechos objeto de debate, en lo que respecta a su naturaleza y contenido<sup>136</sup>.

Conforme al artículo 348 LEC, el órgano judicial valora el dictamen en base a los principios de sano juicio y sana crítica. Todo ello se realizará de manera indirecta, evaluándose la autoridad científica del perito, la aceptabilidad, los métodos científicos aplicados por el perito y sobre todo, la coherencia lógica de argumentación desarrollada por el mismo (STC 228/1997 de 16 de diciembre).

En base a lo anterior, ¿la falta de juramento o promesa de objetividad recogido en el art. 335.2 LEC en los informes periciales parte de un defecto subsanable o constituye un requisito esencial, cuya ausencia priva al informe de valor como prueba pericial? <sup>137</sup>. Inicialmente, la jurisprudencia consideraba que se trataba de un defecto subsanable (SAP de Asturias 31 de octubre de 2023, la SAP de Pontevedra 359/2013, SAP de Madrid 366/2013), argumentando que el juramento del artículo 335.2 LEC es un requisito procesal y que, por lo tanto, su omisión podrá subsanarse mediante la ratificación del perito en el juicio oral, si en ese momento el mismo prestase juramento o promesa<sup>138</sup>.

---

<sup>135</sup> Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil...”, *op. cit.*, pp. 275, 276.

<sup>136</sup> *Ibid.*, pp. 289-290.

<sup>137</sup> Consejo General del Poder Judicial, “Nuevas tecnologías, prueba y protección de datos...”, *op. cit.*, pp. 29–32.

<sup>138</sup> *Id.*

Por otro lado, el criterio establecido por la SAP de Sevilla 307/2012 y por la SAP de Madrid 272/2013 considera que el defecto no es subsanable en base a que el juramento no es un mero formalismo sino una garantía de objetividad. Este criterio fue ratificado por la STS de fecha 11 de enero de 2012 <sup>139</sup> recalcando que el juramento es un requisito esencial y definitorio de la naturaleza del dictamen pericial.

La respuesta final es concluyente, la ausencia de juramento o promesa no es subsanable. El TS concluyó que resulta válido el juramento incluido como “cláusula de estilo” siempre que conste expresamente en el informe.

La metodología empleada para la realización de un peritaje informático es descrita por el perito informático RUBIO ALAMILLO de la siguiente forma: *“Tras un primer contacto inicial con el cliente, el perito procede a realizar un análisis preliminar del problema, considerando los objetivos, el alcance de la investigación y los actores involucrados. Posteriormente, el profesional deberá recopilar todas las evidencias informáticas relevantes para la elaboración del informe, incluyendo portátiles, discos duros, CD-ROMs, DVDs, entre otros. Además, puede ser necesario realizar copias forenses clónicas ante notario de los discos duros o dispositivos de almacenamiento masivo, con el objetivo de preservar la información original y mantener la cadena de custodia. Finalmente, si es requerido, se lleva a cabo la presentación y defensa del informe ante el juez”* <sup>140</sup>

El cumplimiento de la cadena de custodia en una evidencia informática es un tema de una gran complejidad, ya que, para evitar su ruptura, se requiere por parte del perito informático de un profundo conocimiento en materia de análisis forense informático para prevenir la contaminación de la evidencia y de la consecuente impugnación e invalidez del informe<sup>141</sup>. Todo ello queda definido por la STC 170/2003<sup>142</sup> puesto que «la incorporación al proceso penal de los soportes informáticos» debe realizarse «con el cumplimiento de las exigencias necesarias para garantizar una identidad plena e integridad en su contenido con lo intervenido y,

---

<sup>139</sup> Sentencia del Tribunal Supremo, Sala Primera, de 11 de enero de 2012 (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 20 de marzo de 2026.

<sup>140</sup> Rubio Alamillo, J., «Metodología para la realización de un peritaje informático», *Perito Informático Colegiado*, 2014 (disponible en <https://peritoinformaticocolegiado.es/metodologia/>; última consulta 1/03/2026)

<sup>141</sup> Rubio Alamillo, J., «El peritaje informático», *Perito Informático Colegiado*, Madrid, 2014 (disponible en <https://peritoinformaticocolegiado.es/>; última consulta 1/03/2026).

<sup>142</sup> Sentencia del Tribunal Constitucional, Sala Segunda, núm. 170/2003, de 29 de septiembre (recursos de amparo núms. 446/2001, 528/2001 y 655/2001) (versión electrónica-Boletín Oficial del Estado. Ref. BOE-T-2003-19559). Fecha de última consulta: 13 de marzo de 2026.

consecuentemente, que los resultados de las pruebas periciales» se llevan a cabo «sobre los mismos soportes intervenidos o que éstos no hubieran podido ser manipulados en cuanto a su contenido»<sup>143</sup>.

La destrucción de la cadena de custodia en evidencias informáticas puede producirse por diversas causas; entre ellas, el analizar el ordenador sin adoptar las precauciones necesarias. La conexión de dispositivos como memorias USB o discos duros sin la protección adecuada de lectura, genera la pérdida irreversible de la prueba.

Resulta necesario hablar del código hash, una secuencia de caracteres que actúa como una “huella digital” que se obtiene al aplicar una función matemática a un archivo y que permite identificar de forma única el concreto archivo. Si el archivo se modifica, aunque sea un solo carácter, el hash cambia por completo, delatando la manipulación. En consecuencia, cuando es calculado posteriormente resulta necesariamente diferente al obtenido en el momento del volcado inicial (ya que cualquier cambio mínimo en el archivo provocará un cambio en el código hash)<sup>144</sup>. Para que la prueba sea anulada por la ruptura de la cadena de custodia, es imprescindible que dicha pérdida se demuestre de manera absolutamente fehaciente ya que la mera sospecha de interrupción no es suficiente. Así lo establecen las STS 685/2010 y la STS 356/2016 que dictaminan que sólo la certeza absoluta de la interrupción de la cadena de custodia puede invalidar la prueba<sup>145</sup>.

En lo que respecta a las aplicaciones de mensajería instantánea, el perito, para demostrar la ausencia de manipulación de mensajes procedentes de aplicaciones de mensajería instantánea o similares, deberá realizar un examen informático forense. Este análisis debe efectuarse en el dispositivo del emisor o del receptor, en función de dónde se encuentren los mensajes que se quieran autenticar; o si fuese posible en ambos. Si nos encontramos en el primer caso de mensajes recibidos, si el análisis forense determina que no hubo manipulación, entonces, el perito procede a verificar que el dispositivo emisor no fue extraviado ni sustraído, y que, por tanto, los mensajes fueron enviados por su propietario. En consecuencia, debe descartarse

---

<sup>143</sup> Rubio Alamillo, J., “Conservación de la cadena de custodia de una evidencia digital”, *Diario La Ley*, n.º 8859, 9 de noviembre de 2016, Wolters Kluwer, Madrid, p. 3 (disponible en <https://peritoinformaticocolegiado.es/wp-content/uploads/Conservacion-de-la-cadena-de-custodia-de-una-evid....pdf>; última consulta 1/03/2026).

<sup>144</sup> Ibid., pp. 10–11.

<sup>145</sup> Id.

también la posibilidad de que un tercero haya enviado los mensajes suplantando al teléfono emisor utilizando una aplicación informática instantánea<sup>146</sup>.

En consonancia con lo anterior, la única forma de garantizar parcialmente el envío de mensajes por parte del propietario consiste verificar si el teléfono, durante el periodo que se enviaron los mensajes, estaba protegido mediante contraseña o patrón de seguridad. El carácter “parcial” de esta garantía hace referencia a la posibilidad de que algún familiar o persona cercana haya observado el código o patrón y haber sustraído temporalmente el dispositivo para enviar los mensajes. En conclusión, si no es posible realizar el examen del teléfono del emisor, únicamente se dispondrá del análisis pericial del teléfono del receptor, debiendo el juez valorarlo en conjunto con el resto de las pruebas.

Respecto a los mensajes enviados, se debe certificar tanto el envío como la recepción auténtica y descartar así posibles manipulaciones. Sin embargo, aunque se confirme el envío y la recepción, el receptor podría alegar no haber leído los mensajes ya que otra persona pudo haber accedido y eliminado los mensajes antes de que fueran vistos<sup>147</sup>.

En conclusión, en la realidad práctica, es cierto que la verificación de la autenticidad y autoría de los mensajes presenta claras limitaciones técnicas, por lo que la valoración final dependerá del análisis pericial y del resto del conjunto de pruebas. A la hora de emitir un informe pericial sobre correos electrónicos, RUBIO ALAMILLO distingue dos aspectos principales: Primero, la necesidad de diferenciar entre los correos enviados y recibidos, siendo más complicado analizar los enviados ya que al igual que lo que sucede con los mensajes procedentes de aplicaciones de mensajería instantánea, es necesario verificar su autenticidad y la efectiva recepción a su destinatario. Segundo, es relevante considerar e identificar en qué tipo de servidor se almacenan los correos; pueden estar en servidores propios, servidores de proveedores externos o en servicios en la nube como Gmail u Outlook<sup>148</sup>.

---

<sup>146</sup> Rubio Alamillo, J., “Peritaje informático de conversaciones de WhatsApp o aplicaciones similares”, Perito Informático Colegiado, 14 de septiembre de 2014 (disponible en <https://peritoinformaticocolegiado.es/blog/peritaje-informatico-de-conversaciones-de-whatsapp-o-aplicaciones-similares/>; última consulta 22/02/2026).

<sup>147</sup> Id.

<sup>148</sup> Rubio Alamillo, J., “Peritaje informático de correos electrónicos”, Perito Informático Colegiado, 31 de diciembre de 2014 (disponible en <https://peritoinformaticocolegiado.es/blog/peritaje-informatico-de-correos-electronicos/>; última consulta 22/03/2026)

A la hora de analizar la autenticidad del correo recibido, se puede comparar la copia local con la almacenada en el servidor, de lo contrario, el perito debe examinar las cabeceras (conjunto de datos técnicos que acompañan a cada mensaje y que proporcionan información relevante sobre el origen, destino, fecha y hora de envío y recepción, permitiendo rastrear el recorrido del mensaje). Los correos enviados suelen carecer de cabeceras, por lo que su falsificación será más sencilla, y también existe la posibilidad de que no lleguen a su destinatario por diversas causas. Por ello, lo ideal es enviar correos con confirmación de entrega (mensajes procedentes del correo que solicitan al servidor o al destinatario una notificación automática cuando el mensaje ha sido entregado exitosamente en la bandeja de entrada del receptor)<sup>149</sup>.

Si el servidor ha estado bajo control de la parte investigada, se debe analizar para descartar manipulaciones, pero, si pertenece a una empresa externa que cumple con la normativa y estándares propios de una seguridad adecuada, no será necesario un análisis técnico profundo. Por último, si los correos están en servicios en la nube, no es posible acceder directamente a los servidores, por lo que el análisis se limita a lo que puede certificarse desde la propia web, empleando herramientas especializadas<sup>150</sup>. En conclusión, los correos electrónicos aportados como pruebas que no cuenten con el respaldo de un informe pericial profesional son fácilmente impugnables, al no contar con cabeceras ni ningún análisis técnico.

## CONCLUSIONES

Tras haber analizado exhaustivamente cada apartado, la regulación, la doctrina y la jurisprudencia en materia de prueba digital, procedo a dar respuesta a las cuestiones planteadas al inicio de este trabajo así como a formular una serie de propuestas de *lege ferenda* que, a mi juicio, pueden dotarnos de mayor coherencia y seguridad jurídica.

PRIMERA. Resulta necesario un tratamiento diferenciado de la prueba digital. La prueba digital debe tener un tratamiento jurídico distinto del previsto para los medios de prueba tradicionales debido a su carácter volátil, su fácil manipulación y la complejidad técnica que implica su obtención, conservación y análisis dado el riesgo de fundamentar una resolución judicial en elementos fraudulentos.

---

<sup>149</sup> Id.

<sup>150</sup> Id.

SEGUNDA. El marco normativo vigente resulta insuficiente. Se carece de una regulación sistemática y completa de la prueba digital. Ni la LEC ni la LECRIM, pese a las recientes reformas ofrecen una regulación específica y detallada de sus singularidades obligando a los tribunales a realizar una interpretación extensiva de las categorías clásicas para suplir las lagunas normativas caso por caso, sentando los criterios aplicables.

TERCERA. La cadena de custodia y la prueba pericial informática se conforman como garantías esenciales. Ante la fácil manipulación de los archivos digitales, la prueba pericial informática se convierte en la herramienta esencial para garantizar la evidencia. La pericial permite verificar la autoría, la fecha de su creación y certifica la corrección de la cadena de custodia mediante protocolos específicos (como el uso de bloqueadores de escritura o los códigos hash) que permiten que se determine si la misma forme parte del acervo probatorio o pierda su eficacia.

CUARTA. Los derechos fundamentales son un límite infranqueable en la obtención de la prueba digital. Debe realizarse con respeto a los derechos fundamentales, el derecho a la intimidad personal y familiar (art. 18.1 CE) y el secreto de las comunicaciones (art. 18.3 CE). La doctrina constitucional y la jurisprudencia han establecido que las comunicaciones digitales aportadas por uno de los interlocutores son lícitas. El acceso a dispositivos ajenos y la interceptación de comunicaciones sin autorización judicial ni consentimiento determinan la ilicitud de la prueba y su expulsión del proceso.

QUINTA. Resulta necesaria una ley integral de la prueba digital. Una norma unitaria que regule las especificidades de la prueba digital en los procesos judiciales articulada como una ley orgánica complementaria de las leyes procesales y que establezca un marco común que otorgue seguridad jurídica a y criterios uniformes incorporando:

1. La definición y clasificación legal de la prueba digital, atendiendo a su naturaleza y las particularidades de su tratamiento procesal.
2. La regulación de la obtención lícita de la prueba.
3. El establecimiento de un estándar para la cadena de custodia, indicando los requisitos mínimos que debe cumplir.

4. Una configuración legal de la prueba pericial informática, definiendo los requisitos de titulación y especialización de los peritos, el contenido de sus dictámenes y los estándares técnicos homologados exigibles.
5. La admisión de sistemas de certificación tecnológica tipo actas notariales digitales o plataformas de certificación electrónica, agilizando el proceso y reduciendo costes.
6. Un régimen de impugnación y valoración específico en función de las garantías que la acompañen.
7. La previsión de mecanismos que faciliten el acceso a la prueba pericial informática en condiciones de igualdad, arbitrando sistemas de asistencia pericial gratuita en aquellos casos en que la prueba resulte esencial para la defensa y su coste pudiera resultar desproporcionado en garantía de la tutela efectiva y el acceso garantizado a la justicia.

Considero que la creación de una ley integral de la prueba digital es una asignatura pendiente de nuestro legislador para hacer frente a los desafíos que plantea la actual sociedad digital.

## **BIBLIOGRAFÍA**

### **Legislación**

Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE 17 de septiembre de 1882).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 8 de enero de 2000).

Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DOUE 28 de agosto de 2014).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018).

### **Jurisprudencia**

Sentencia del Tribunal Supremo, Sala de lo Penal, núm. 754/2015, de 27 de noviembre (versión electrónica-base de datos VLEX). Fecha de última consulta: 1 de febrero de 2026.

Sentencia del Tribunal Supremo, Sala Primera, núm. 275/2011, de 28 de abril (recurso núm. 1083/2007) (versión electrónica-base de datos del Tribunal Supremo). Fecha de última consulta: 7 de febrero de 2026.

Sentencia de la Audiencia Provincial de Baleares, Sección 5.ª, núm. 352/2012, de 23 de julio, recurso núm. 187/2012, (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 8 de febrero de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 300/2015, de 19 de mayo (versión electrónica-base de datos VLEX). Fecha de última consulta: 8 de febrero de 2026

Sentencia del Tribunal Supremo, Sala Primera, núm. 1190/2009, de 3 de diciembre (versión electrónica-base de datos VLEX). Fecha de última consulta: 9 de febrero de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 587/2014, de 18 de julio (versión electrónica-base de datos VLEX) Fecha de última consulta: 10 de febrero de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 287/2017, de 19 de abril (versión electrónica-base de datos VLEX). Fecha de última consulta: 10 de febrero de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 489/2018, de 23 de octubre (recurso de casación núm. 1674/2017) (versión electrónica-base de datos VLEX). Fecha de última consulta: 1 de febrero de 2026

Sentencia del Tribunal Supremo, Sala Quinta, núm. 114/2017, de 21 de noviembre (versión electrónica-base de datos VLEX). Fecha de última consulta: 1 de marzo de 2026.

Sentencia del Tribunal Superior de Justicia de Cantabria, de 11 de diciembre de 2017 (recurso núm. 859/2015) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 18 de marzo de 2026

Sentencia del Tribunal Superior de Justicia de Islas Canarias, de 16 de abril de 2018 (recurso núm. 799/2017) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 1 de febrero de 2026.

Sentencia del Tribunal Superior de Justicia de Asturias, de 26 de diciembre de 2019 (recurso núm. 2232/2019) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 10 de marzo de 2026.

Sentencia del Tribunal Superior de Justicia de Galicia, de 27 de enero de 2016 (recurso núm. 556/2016) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 7 de marzo de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 119/2019, de 6 de marzo (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 12 de marzo de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 375/2018, de 19 de julio versión electrónica-base de datos CENDOJ). Fecha de última consulta: 12 de marzo de 2026.

Sentencia del Tribunal Supremo, Sala Segunda, núm. 706/2020, de 23 de julio (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 1 de febrero de 2026.

Auto del Tribunal Supremo, Sala Segunda, núm. 2501/2013 (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 13 de marzo de 2026.

Sentencia del Tribunal Constitucional, núm. 34/1996, de 11 de marzo (versión electrónica-base de datos del Tribunal Constitucional). Fecha de última consulta: 1 de febrero de 2026.

Sentencia de la Audiencia Provincial de Lleida, Sección 2.<sup>a</sup>, núm. 411/2022, de 17 de junio (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 9 de marzo de 2026.

Sentencia del Tribunal Supremo (Sala Primera), de 11 de enero de 2012 (ROJ: STS 235/2012) (versión electrónica-base de datos CENDOJ). Fecha de última consulta: 20 de marzo de 2026.

Sentencia del Tribunal Constitucional, Sala Segunda, núm. 170/2003, de 29 de septiembre (recursos de amparo núms. 446/2001, 528/2001 y 655/2001) (versión electrónica-Boletín Oficial del Estado. Ref. BOE-T-2003-19559). Fecha de última consulta: 13 de marzo de 2026.

Sentencia del Tribunal Supremo (Sala Quinta, de lo Militar), núm. 82/2018, de 15 de octubre) (versión electrónica-base de datos vLex). Fecha de última consulta: 2 de marzo de 2026.

### **Obras doctrinales**

Abel Lluch, F. J., “El documento electrónico: acceso, impugnación y valoración” en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 46, Madrid, 2022, pp. 6-8 y 12-17.

Alemany Eguidazu, J., “La prueba de la autenticidad electrónica con la LEC”, *Poder Judicial. Nueva Época*, n.º 1, 2002, cap. III, apartado 2 (Medios probatorios con la nueva Ley de Enjuiciamiento Civil).

Arbós y Llobet, R., “La prueba electrónica”, Bosh, Barcelona, 2011, pp. 348 y ss.

Consejo General del Poder Judicial, “La prueba en el proceso civil, la prueba ilícita y la prueba generada en el seno de las nuevas tecnologías: conclusiones”, *Cuadernos Digitales de Formación*, n.º 24, Madrid, 2018, pp. 4-7, 29-33 y 65-68.

Consejo General del Poder Judicial, “Los nuevos problemas de la prueba en el proceso civil. La prueba electrónica”, *Cuadernos Digitales de Formación*, n.º 46, Madrid, 2022, pp. 9-12.

Consejo General del Poder Judicial, “Nuevas tecnologías, prueba y protección de datos: conclusiones”, *Cuadernos Digitales de Formación*, n.º 72, Madrid, 2021, pp. 5–8.

Cortés Domínguez, V. y Moreno Catena, V., “Derecho Procesal Civil. Parte General” (14.<sup>a</sup> ed.), *Tirant lo Blanch*, Valencia, 2025, pp. 275-279.

De Miranda Vázquez, C., “Prueba directa vs. prueba indirecta (Un conflicto inexistente)”, *Doxa. Cuadernos de Filosofía del Derecho*, Alicante, n.º 38, 2015, pp. 73-100.

De Urbano Castrillo, E., “La valoración de la prueba electrónica”, *Tirant lo Blanch*, Valencia, 2009, p. 47.

Delgado Martín, J., “La prueba digital. Concepto, clases, aportación al proceso y valoración”, *Sección Ciberderecho, Diario La Ley*, n.º 6, 2017, pp. 13.

Delgado Martín, J., “Estándares probatorios en la prueba digital”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 46, Madrid, 2022, pp. 6-17 y 30-35.

De Miranda Vázquez, C., “Prueba directa vs. prueba indirecta (Un conflicto existente)”, n.º 38, 2015, pp. 76–77.

Díaz Pita, M.<sup>a</sup> P., “Digitalización de la Justicia: prevención, investigación y enjuiciamiento”, en *Estudios*, Aranzadi, Navarra, 2022.

Díez-Picazo Giménez, L.M., “Sistema de Derechos Fundamentales”, Civitas, Madrid, 2008.

Tapia Fernández, I., “Comentario al artículo 217 de la Ley de Enjuiciamiento Civil”, en *Comentarios a la Ley de Enjuiciamiento Civil*, colección Grandes Tratados, Aranzadi, Navarra, 2001.

García Pérez, M. F., “Nuevas tecnologías y derechos humanos: análisis de las grabaciones en el proceso penal”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 19, Madrid, 2022, pp. 9-14, 29-31.

García Martín, J. A. et al., “Administración electrónica. Aspectos jurídicos organizativos y técnicos”, Thomson Reuters Aranzadi, Navarra, 2021, p. 2.

Garcimartín Montero, R., “Comentario al artículo 294 de la Ley de Enjuiciamiento Civil”, en *Comentario a la Ley de Enjuiciamiento Civil*, tomo I, Aranzadi, Navarra, 2011.

Garrido Carrillo, F. J., *Principios y garantías del proceso penal de menores*, Aranzadi, Navarra, 2023.

González Granda, P., “La valoración de la prueba”, en Romero Pradas, S. y González Cano, M. I. (coords.), *La prueba*, Aranzadi, 2017.

Gómez Montoro, Á. J., “Jurisdicción constitucional y judicial en el recurso de amparo”, Tirant lo Blanch, Valencia, 2006.

Gómez Montoro, Á. J., “Capítulo II: Los derechos procesales del artículo 24 CE”, en Gómez Montoro, Á. J., *Jurisdicción constitucional y judicial en el recurso de amparo*, Tirant lo Blanch, Valencia, 2006.

López Hormeño, M. del C., “Las fuentes de obtención de la prueba tecnológica: los correos electrónicos, el WhatsApp y las redes sociales”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 32, 2022, pp. 9-14

Lloria García, P., “Infancia, adolescencia y nuevas tecnologías según la Ley Orgánica 8/2021 ”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación*, n.º 17, Madrid, 2022, pp.5-7

Mas Carrillo, M., “Proceso laboral: prueba digital y protección de datos. Aspectos procesales”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 13, Madrid, 2020, pp. 36-37.

Montero Aroca, J., “Las cintas magnetofónicas como fuentes de prueba (Comentario a la Sentencia del Tribunal Supremo, Sala I, de 30 de noviembre de 1981”, *Poder judicial*, 1983-1, p.40, para quien el empleo de grabaciones magnetofónicas, vídeos, fotografías, películas, etc, en el proceso civil era, justamente, reflejo del derecho al uso de los medios de prueba pertinentes para la defensa tal y como proclama el art. 24 de la Constitución.

Muñoz Aranguren, A., “El tratamiento de la prueba ilícita por la reciente jurisprudencia de la Sala Segunda del TS: algunas tendencias”, *Revista Aranzadi de Derecho y Proceso Penal*, n.º 77, 2025.

Orellana Cano, N. A., “La prueba en el tráfico mercantil ”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 50, Madrid, 2009, pp. 26-37

Ortuño Navalón, M.<sup>a</sup> del Carmen, “Aspectos procesales de la prueba electrónica”, en Ortuño Navalón, M.<sup>a</sup> del Carmen, *La prueba electrónica ante los tribunales*, Tirant lo Blanch, Valencia, 2014.

Pérez Asenjo, A. I., “Registro físico y remoto de dispositivos de almacenamiento masivo y sistemas informáticos”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 59, pp. 15-17, 39.

Rivas Velasco, M. J., “Documento electrónico: medios e instrumentos de reproducción de la palabra, sonido e imagen”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 24, Madrid, 2018, pp. 3-12.

Sanchís Crespo, C., “La prueba en soporte electrónico”, en AA.VV., *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, Thomson Reuters Aranzadi, Navarra, 2012, pp.713.

Suárez Robledano, J. M., “La relevancia de la prueba electrónica en la lucha contra los delitos informáticos”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 52, Madrid, 2009, pp. 9-11.

Tardón Olmos, M., “La violencia de género a través de las nuevas tecnologías”, en Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 37, Madrid, 2017, pp.17-20.

Troncoso Reigada, A., “La protección de datos personales. En busca del equilibrio”, Tirant lo Blanch, Valencia, 2010, p. 110-115.

Urbano Castrillo, E. de y Torres Morato, M. A., *La prueba ilícita penal: estudio jurisprudencial*, Aranzadi, Navarra, 2003, pp. 47.

Velasco Núñez, E., “Correo electrónico, SMS y “virus troyanos”: aspectos procesales penales”, Consejo General del Poder Judicial, *Cuadernos Digitales de Formación* n.º 22, Madrid, 2009, p. 26-27.

#### Recursos de Internet

Rubio Alamillo, J., “Conservación de la cadena de custodia de una evidencia digital”, *Diario La Ley*, n.º 8859, 9 de noviembre de 2016, Wolters Kluwer, Madrid, p. 3 (disponible en <https://peritoinformaticocolegiado.es/wp-content/uploads/Conservacion-de-la-cadena-de-custodia-de-una-evid....pdf>; última consulta 1/03/2026).

Ibáñez Rodríguez, A., “El derecho a la prueba como garantía esencial del proceso”, *Hay Derecho*, entrada de 9 de junio de 2025 (disponible en <https://www.hayderecho.com/2025/06/09/el-derecho-a-la-prueba-como-garantia-esencial-del-proceso/>; última consulta 15/03/2026).

Rubio Alamillo, J., «El peritaje informático», *Perito Informático Colegiado*, Madrid, 2014 (disponible en <https://peritoinformaticocolegiado.es/>; última consulta 1/03/2026).

Pasamar, A., “La prueba pericial informática frente a la impugnación de la autenticidad de un e-mail”, 2011 (disponible en <http://www.esade.edu/itemsweb/content/produccion/4010660.pdf>; última consulta 26 de febrero de 2026).

Rubio Alamillo, J., «Metodología para la realización de un peritaje informático», *Perito Informático Colegiado*, 2014 (disponible en <https://peritoinformaticocolegiado.es/metodologia/>; última consulta 1/03/2026)

Rubio Alamillo, J., “Peritaje informático de correos electrónicos”, *Perito Informático Colegiado*, 31 de diciembre de 2014 (disponible en <https://peritoinformaticocolegiado.es/blog/peritaje-informatico-de-correos-electronicos/>; última consulta 22/03/2026).

Rubio Alamillo, J., “Peritaje informático de conversaciones de WhatsApp o aplicaciones similares”, *Perito Informático Colegiado*, 14 de septiembre de 2014 (disponible en <https://peritoinformaticocolegiado.es/blog/peritaje-informatico-de-conversaciones-de-whatsapp-o-aplicaciones-similares/>; última consulta 22/02/2026).

Rubio Alamillo, J., “Adquisición y presentación en un procedimiento judicial de una prueba informática”, *El Derecho*, 4 de abril de 2017 (disponible en <https://elderecho.com/adquisicion->

[y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica?utm\\_source](#); última consulta 18/03/2026).

Beltrán Pardo, A. I., “Los contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo”, Noticias Jurídicas, 30 de septiembre de 2015 (disponible en <https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533-las-contenidos-de-whatsapp-como-medio-probatorio-en-el-ambito-de-las-diligencias-urgente/>; última consulta 10/03/2026).