



FACULTAD DE DERECHO

LA PRUEBA DIGITAL EN EL PROCESO CIVIL

Verificación y régimen general

Autor: Mercedes Olmos García

4º, E-1 Business Law

Área de Derecho Procesal

Tutor: Luis F. Bermejo Reales

Madrid

Abril de 2017

ANEXO III

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DEL TFG

Nombre y apellidos del alumno:

Mercedes Olmos García

Curso y Especialidad: 4º Grado Derecho y Diploma en Business Law (E-1)

Declaro, bajo mi responsabilidad, que el Trabajo de Fin de Grado presentado con el título “La prueba digital en el proceso civil. Verificación y régimen general” en la Facultad de Derecho de la Universidad Pontificia Comillas en el curso académico 2017-2018 :

1º.- Es un trabajo de mi autoría, original, inédito y no ha sido presentado con anterioridad a otros efectos.

2º.- Cumple con todos los requerimientos generales anti-plagio aplicables para la elaboración de trabajos académicos en la Universidad Pontificia Comillas y se ajusta a las buenas prácticas existentes sobre el particular.

Madrid, ade..... de.....

Fdo.:

RESUMEN

El objeto del presente trabajo es el de analizar la prueba digital o electrónica en el proceso civil. Más concretamente, nos centraremos en la incorporación de ésta al proceso y en su verificación y conservación a través de la prueba pericial y la cadena de custodia, pues ambas juegan un papel fundamental en cuanto a evitar la fácil manipulación y falsificación a la que estas pruebas están expuestas. Nuestro ordenamiento jurídico no contiene aún una regulación expresa para la prueba electrónica, a pesar de la asiduidad con la que, en la sociedad actual, los hechos relevantes para un proceso judicial necesitan ser probados por esta vía. Hablamos de incorporar al proceso correos electrónicos, mensajes de texto (SMS), o WhatsApp mediante medios de prueba como un documento en soporte papel, tomando como ejemplo los *pantallazos* que hacemos con nuestros teléfonos móviles; o un documento electrónico mediante un *pen drive* o un CD. Por supuesto, el resto de medios de prueba tradicionales tienen su campo de aplicación también en este ámbito. Otro de los ejes del trabajo que a continuación se propone es el de analizar la estrecha relación existente entre la obtención de la prueba digital y la vulneración de determinados derechos fundamentales. Haciendo especial alusión a los derechos a la intimidad, a la protección de datos y al secreto de las comunicaciones, se puede entender que habrá que tratar con especial cautela la manera de obtención de dichas pruebas para que puedan ser tomadas en consideración por el órgano jurisdiccional competente.

PALABRAS CLAVE

Proceso civil, prueba digital, verificación, medios de prueba, redes sociales, autenticidad.

ABSTRACT

The main purpose of this study is the analysis of the digital proof in civil judicial proceedings. We will analyse more deeply how this type of proof is presented in a judicial proceeding and its conservation and process of verification throughout an expert report and the chain of custody. These two tools play a vital role when it comes to avoiding manipulation and forgery, which are, nowadays, truly easy to do in digital proof. Surprisingly, our legal system does not have specific regulation for this type of proof, even if we take into account that in today's society the relevant facts to prove in a trial may need this type of proof to be taken into account. We are referring to e-mails, texts or WhatsApp messages being used as evidence in a trial and presented to the court throughout paper document, for example, when we take a screen-shot of a text message; or throughout an electronic document, in this case we shall use a pen-drive or a CD. Another key element of this study is the relation between the way we can obtain digital proof and the violation of fundamental rights. Making special emphasis on the right to privacy and secrecy of communication as well as to the right to data protection, we may point out that the way the digital proof is collected will have to be treated with special care and caution so as to avoid illegality of proof and to have the court consider those pieces of information as part of the trial.

KEY WORDS

Civil trial, digital proof, verification, sources of proof, social networks, authenticity.

ÍNDICE

INTRODUCCIÓN.....	9
1. INTRODUCCIÓN A LA PRUEBA EN EL PROCESO CIVIL	11
1.1. La distinción entre fuentes y medios de prueba	12
1.2. Principales medios de prueba	13
2. LA PRUEBA DIGITAL O ELECTRÓNICA.....	17
2.1. Introducción y concepto	17
2.2. Naturaleza de la prueba digital o electrónica	19
2.3. Normativa aplicable.....	20
2.3.1. <i>Ámbito internacional.....</i>	<i>21</i>
2.3.2. <i>Ámbito de la Unión Europea.....</i>	<i>21</i>
2.3.3. <i>Ámbito nacional</i>	<i>22</i>
2.4. Principales medios de prueba digital	23
2.5. Principales fuentes de prueba digital	25
2.5.1. <i>Correo electrónico</i>	<i>25</i>
2.5.2. <i>Páginas web</i>	<i>26</i>
2.5.3. <i>Mensajes de teléfono móvil (SMS)</i>	<i>27</i>
2.5.4. <i>WhatsApp y otros medios de mensajería instantánea</i>	<i>28</i>
2.5.5. <i>Redes sociales.....</i>	<i>31</i>
3. LA PRUEBA DIGITAL O ELECTRÓNICA EN EL PROCESO. ESPECIAL REFERENCIA AL PROCESO CIVIL	35
3.1. Proposición de la prueba digital y momento de aportación.....	35
3.2. Obtención de la prueba digital.....	36
3.2.1. <i>Información contenida en un dispositivo electrónico</i>	<i>36</i>
3.2.2. <i>Información transmitida por vía digital.....</i>	<i>37</i>
3.3. Incorporación al proceso de la prueba digital.....	38
3.3.1. <i>¿A través de qué medios de prueba se puede incorporar al proceso la prueba digital?</i>	<i>39</i>
3.3.2. <i>Otros requisitos para la aportación.....</i>	<i>43</i>
3.3.3. <i>Conservación y verificación.....</i>	<i>44</i>
3.4. Admisión de la prueba digital	49

3.5. Práctica de la prueba digital	50
3.6. Valoración de la prueba digital.....	51
4. LICITUD E ILICITUD DE LA PRUEBA DIGITAL. ALUSIÓN A DETERMINADOS	
DERECHOS FUNDAMENTALES	52
4.1. El derecho a la intimidad personal y familiar	53
4.2. El derecho de secreto de las comunicaciones.....	57
4.3. La protección de datos personales	58
4.4. La prueba digital ilícita	61
CONCLUSIONES	63
BIBLIOGRAFÍA.....	65

ABREVIATURAS

Art.	Artículo
ATC	Auto del Tribunal Constitucional
ATS	Auto del Tribunal Supremo
CC	Código Civil
CE	Constitución Española de 1978
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
LEC	Ley de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal
LFE	Ley de la Firma Electrónica
LOPD	Ley Orgánica de Protección de Datos

LOPJ	Ley Orgánica del Poder Judicial
SAP	Sentencia de la Audiencia provincial
SMS	Short Message Service
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo
UE	Unión Europea
UNCITRAL	Comisión de las Naciones Unidas para el derecho mercantil

INTRODUCCIÓN

Hoy en día vivimos en un mundo en el que las redes de comunicación social y las nuevas tecnologías se han convertido en la piedra angular de nuestras relaciones sociales. La sociedad en la que vivimos se conoce como “sociedad de la información”, expresión que se ha popularizado y incluso por instituciones como la Comisión Europea, como se demuestra en la Directiva 2000/31/CE. Bajo el nombre “sociedad de la información” se engloban todos los servicios de las Tecnologías de la Información y las Comunicaciones, las hoy conocidas como TIC.

Las nuevas tecnologías e Internet – “interconnected networks” o redes interconectadas – son las redes de comunicación que permiten a los usuarios el intercambio casi instantáneo de información a nivel mundial y suponen la mejor herramienta para obtener información y datos sobre cualquier área, los cuales, no dejan de aumentar convirtiéndose casi en ilimitados¹. La Directiva 2002/58/CE dice que *“Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad”*².

Internet, las redes sociales o los nuevos medios de comunicación como SMS, WhatsApp o Skype son tanto un mecanismo de propagación global de información como un medio de interacción entre individuos, independientemente del lugar en el que se encuentren. “En la actualidad, según datos publicados por el Banco Mundial, el 46% de la población mundial es usuaria de Internet.”³

¹ Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p. 13.

² Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

³ Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p. 13,14.

Hoy en día, en nuestro entorno, cada persona cuenta, al menos, con dos dispositivos electrónicos: un teléfono móvil con acceso a internet y un ordenador. En los últimos años hemos sido testigos del considerable incremento de dispositivos móviles y conexiones móviles inteligentes: “a nivel mundial, se espera que éstos en solo tres años, en 2020, supongan el 72% del total, siendo ‘tan sólo’ el 36% en 2015.” Según el Instituto Nacional de Ciberseguridad, en 2020 habrá más de 25 millones de Apps, más de 25 billones de sistemas integrados e inteligentes y 50 trillones de Gbs de datos⁴.

El sistema judicial no puede quedarse atrás ante estos avances y debe aceptar que cada vez son más los hechos en los que está presente algún medio de información en forma electrónica que la persona genera con su actividad diaria. Las aplicaciones de mensajería instantánea destacando la ya mencionada WhatsApp, los correos electrónicos, las bases de datos, el historial de navegación de Internet o los registros de transacciones en cajeros automáticos son sólo algunos de los muchos ejemplos en los que día a día, de manera automática y cotidiana, una persona va depositando información que, de cara a un proceso judicial, puede constituir una fuente de prueba esencial para demostrar la veracidad de sus argumentos⁵.

Así, quise emplear esta oportunidad de investigación y análisis, el Trabajo de Fin de Grado, para aprender más sobre algo tan actual y necesario hoy en día en el mundo del derecho. Este tema ha suscitado muchas preguntas a lo largo del estudio de la asignatura de Derecho Procesal en muchos de mis compañeros y en mí misma. Así pues, decidí adentrarme en esta materia tan novedosa e interesante. Considero que el mundo del derecho en general y los procesos judiciales en particular deben avanzar de manera paralela con las nuevas tecnologías. Esto responde a una doble exigencia: no sólo por la necesidad de adecuarse a los medios de comunicación y la realidad actuales, sino también para lograr una mejora en la eficiencia e informatización de nuestros órganos jurisdiccionales.

⁴ Cisco VNI Mobile 2016, “Internet y fundamentos de informática: servicios, terminología y conceptos”, INCIBE (Instituto Nacional de Ciberseguridad).

⁵ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 35-40.

1. INTRODUCCIÓN A LA PRUEBA EN EL PROCESO CIVIL

La prueba es la actividad procesal que tiende a verificar las afirmaciones de hecho que realizan las partes y que, además, trata de lograr el convencimiento del juzgador.

El objeto de la prueba son las realidades que pueden ser probadas. Por lo general, se puede decir que el objeto de la prueba son los hechos, y en base al artículo 281.1 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 8 de enero de 2000) (en lo sucesivo, LEC) podemos dar una definición más completa de lo que sería el objeto de la prueba: “*La prueba tendrá como objeto los hechos que guarden relación con la tutela judicial que se pretenda obtener en el proceso*”. El objeto de la prueba vendrá determinado por las alegaciones que realicen las partes, generalmente fácticas, aunque cabe prueba del Derecho, por ejemplo, en el caso del Derecho extranjero.

Las alegaciones de hechos son el sustento fundamental de la prueba. Con ellas nos referimos a las afirmaciones de hechos que realicen las partes acerca de los acontecimientos que constituyen el supuesto base de la norma cuya aplicación se pide. No todos los hechos deben de ser probados, pues existen algunos que están exentos de la necesidad de ser probados, nos encontramos con una serie de excepciones: los hechos admitidos o no controvertidos, los hechos notorios y, por último, los hechos favorecidos por una presunción.

En primer lugar, en cuanto a los hechos admitidos, cabe decir que la prueba ha de versar sólo sobre los hechos controvertidos y no sobre aquellos respecto a los cuales ambas partes están conformes. En segundo lugar, los hechos notorios serían aquellos, siguiendo al jurista italiano Piero CALAMANDREI, que “deberían ser conocidos por un hombre con una cultura de grado medio”. La última de las excepciones la constituyen los hechos favorecidos por una presunción. Encontramos, llegados a este punto, cierta controversia doctrinal⁶. En las presunciones legales existen indicios y un hecho

⁶ Controversia doctrinal sobre los hechos favorecidos por una presunción: parte de la doctrina incluye dentro de las excepciones de hechos que no es necesario probar los hechos favorecidos por una presunción legal. Sin embargo, es preciso aclarar esto: en las presunciones legales existen uno o varios indicios y un hecho presumido. La Ley establece que una vez que se prueba el indicio, se presume que el hecho presumido existe por lo que no necesitaría ser probado. Un ejemplo: procedería la declaración de fallecimiento de los tripulantes y pasajeros de una nave naufragada de quienes no se han tenido noticias después de comprobarse el naufragio. El art. 194.2 CC dice que se presumiría ocurrido el

presumido. La ley dice que una vez se prueba o se admite ese indicio, se presume que el hecho presumido existe. Por tanto, no haría falta probarlo. Por otro lado, las presunciones legales *iuris tantum* admiten prueba en contrario; sin embargo más que de exención de prueba hablaríamos de norma especial sobre la carga de la prueba.

A continuación, explicaremos las alegaciones de derecho. Partimos de la base de que, de acuerdo con el principio *iura novit curia*, el conocimiento de la norma jurídica es una de las obligaciones del juzgador. Los tribunales deben resolver conforme a las normas aplicables al caso, así lo establece la Ley de Enjuiciamiento Civil en su artículo 218.1, II. Por tanto, podemos decir que el Derecho no se debe probar, a excepción del Derecho extranjero que sí debe ser objeto de prueba.

1.1. La distinción entre fuentes y medios de prueba

Es necesario precisar la distinción entre las fuentes y los medios de prueba para así poder adentrarnos en el tema que nos ocupa: la prueba digital o electrónica.

De manera simple se puede decir que las fuentes son elementos anteriores al proceso y que existen en la realidad, es decir, la realidad que se quiere probar mediante la actividad o el instrumento, que permite justificar los hechos aseverados o refutados. Serían fuentes, por tanto, los soportes en los que las palabras, las imágenes o los sonidos que se encuentran incorporados y que a través de una prueba electrónica, se puedan emplear en el proceso para probar algo ante el tribunal. Podemos añadir que es a través de los medios de prueba cuando éstas se incorporan al proceso⁷.

Todo lo que gira en torno al proceso está sujeto al principio de legalidad. De este modo, los medios y las fuentes admitidos son aquellos expresados en la ley y deberán proponerse y practicarse según los preceptos legales de modo que la las partes y el Tribunal deberán estar a la regulación que rige la actividad probatorio.

nafragio si el buque no llegara a su destino. Por tanto, se puede probar que el naufragio existe (prueba directa) o que el buque no ha llegado a su destino (prueba indiciaria). La diferencia está en el tema a probar, no en que haya exención de prueba en el segundo caso.

⁷ Montero Aroca J, Gómez Colomer JL, Barona Vilar S, Calderón Cuadrado MP; *Derecho Jurisdiccional II Proceso Civil*, Tirant Lo Blanch; Valencia, 2014, p. 234-236.

1.2. Principales medios de prueba

Si acudimos al artículo 299 LEC⁸ encontraremos la enumeración de los distintos medios de prueba admitidos en nuestro Derecho positivo.

Podemos clasificar los medios de prueba en medios de prueba clásicos o tradicionales (apartado 1 del art. 299 LEC); los medios de prueba modernos o actuales que serían los audiovisuales e informáticos (apartado 2 del art. 299 LEC); y, por último, los medios de prueba futuros que se corresponderían con el tercer apartado del ya mencionado artículo y que deja abierta la posibilidad de incorporar otros medios que no se incluyan en el precepto por ejemplo, porque se desconozcan en la actualidad.

1.2.1. Interrogatorio de las partes y de testigos

En primer lugar, el interrogatorio de testigos o prueba testifical es un medio concreto de prueba (art.299.1,6ª LEC), en virtud del cual una persona ajena al proceso aporta al mismo una declaración sobre hechos presenciados (vistos u oídos) por ella o que ha sabido de referencia. Sobre esos hechos, dicha persona será interrogada, a condición de que esos hechos sean controvertidos y se refieran al objeto del proceso (art. 360 LEC). Es una prueba de naturaleza personal. El testigo será una persona física que sea ajena al proceso, puesto que si tuviera la condición de parte, se sometería a la prueba del interrogatorio de las partes. Asimismo, puede ser testigo una persona jurídica o entidad pública en virtud del art. 381 LEC. En estos casos, responderán por escrito

⁸ Art. 299 LEC: “1. Los medios de prueba de que se podrá hacer uso en juicio son:

- 1.º Interrogatorio de las partes.
- 2.º Documentos públicos.
- 3.º Documentos privados.
- 4.º Dictamen de peritos.
- 5.º Reconocimiento judicial.
- 6.º Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.”

sobre los hechos y en la proposición de prueba habrá de constar con precisión aquello sobre lo que deberá tratar la declaración o informe escrito.

Por tanto, el interrogatorio de las partes litigantes sería la declaración efectuada por las partes sobre los hechos que guarden relación con el objeto del proceso o que tengan incidencia en éste. Más concretamente será la declaración recabada judicialmente por una parte litigante. El art. 301.1 LEC dice que “cada parte podrá solicitar del tribunal el interrogatorio de las demás sobre hecho y circunstancias de los que tengan noticia y que guarden relación con el objeto del juicio. Un colitigante podrá solicitar el interrogatorio de otro colitigante siempre y cuando exista en el proceso oposición o conflicto de intereses entre ambos”.

1.2.2. La prueba documental

La prueba documental es aquella que consiste en la incorporación de la información que se quiere probar a través de un documento público o privado.

Los documentos públicos son, según el art. 1216 CC, “los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley”. Normalmente, se deben aportar al proceso mediante copia auténtica, certificación o testimonio, según tengan naturaleza notarial, administrativa o judicial, respectivamente. El original quedará en el protocolo correspondiente. Los documentos privados serán, por tanto, aquellos en los que no intervenga un funcionario público. En este caso, si se presenta el documento original a pesar de que pueda presentarse copia autenticada por un fedatario público o copia simple aunque a riesgo de disminuir su valor probatorio.

El procedimiento probatorio es muy sencillo en este caso. Simplemente, consistirá en que la parte proponente de esta prueba presente el documento. Sin embargo, puede darse el caso de que el documento en cuestión esté en manos de la parte contraria o de un tercero ajeno al proceso. La situación de acceder al documento, en manos del litigante contrario o de un tercero, por parte de quien pretende introducirlo en el proceso se asemeja a lo contemplado en este art. 265.2 LEC: “*sólo cuando las partes, al presentar su demanda o contestación, no puedan disponer de los documentos,*

medios e instrumentos a que se refieren los tres primeros números del apartado anterior, podrán designar el archivo, protocolo, o lugar en que se encuentren, o el registro, libro registro, actuaciones o expediente del que se pretenda obtener una certificación". El litigante, en lugar de designar el archivo u otro registro en que se halle el documento, podría advertir que se encuentra en poder de la parte contraria. En virtud del art. 330.1 LEC, si el documento se hallare en manos de un tercero ajeno al proceo, se le requerirá la exhibición de documentos de su propiedad cuando, a petición de alguna de las partes, el tribunal entienda que si conocimiento es relevante.

1.2.3. La prueba pericial

El dictamen de peritos o prueba pericial es un medio concreto de prueba a través de la cual una persona con conocimientos especializados (científicos, artísticos, técnicos...) que el juez no tiene y que es ajena al proceso aporta dichos conocimientos para que el órgano jurisdiccional pueda valorar mejor los hechos/circunstancias y adquirir certeza sobre ellos.

La prueba pericial es, como la testifical, una prueba de naturaleza personal puesto que una persona – el perito, que bien puede ser una persona física, o una persona jurídica como viene indicado en los apartados 2º y 3º del art. 340 LEC⁹ – dictamina e informa al juez. Esta persona, el perito, es un tercero o persona ajena al proceso que posee unos conocimientos especializados (tenga o no título profesional) y que los vierte en el proceso tras haberlos aplicado al estudio de los hechos u otros elementos objeto de prueba.

Respecto al procedimiento probatorio en concreto, son las partes las que llaman al perito puesto que sobre ellas recae la carga de alegar y probar la veracidad de los hechos relevantes en que se funda su pretensión o resistencia. Siguiendo lo establecido por el art. 339 LEC en sus apartados 2º, 4º y 5º, las partes pueden pedir la

⁹ Art 340 LEC: **2.** Podrá asimismo solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia. También podrán emitir dictamen sobre cuestiones específicas las personas jurídicas legalmente habilitadas para ello.

3. En los casos del apartado anterior, la institución a la que se encargue el dictamen expresará a la mayor brevedad qué persona o personas se encargarán directamente de prepararlo, a las que se exigirá el juramento o promesa previsto en el apartado segundo del artículo 335.

designación judicial de perito si lo creen conveniente. El tribunal podrá ordenar la prueba pericial de oficio en los casos de declaración o impugnación de la filiación, paternidad y maternidad, en procesos sobre la capacidad de las personas o en procesos matrimoniales¹⁰.

Los dictámenes de que los litigantes dispongan, elaborados por los peritos que ellos han designado, se aportarán con la demanda o la contestación.

Si no es así y el actor/demandado no puede aportar los dictámenes con la contestación/demanda, los aportará 5 días antes de la audiencia previa (juicio ordinario) o de la vista (juicio verbal).

1.2.4. La prueba de reconocimiento judicial

El reconocimiento judicial es otro de los medios de prueba contemplados en la LEC. Procederá cuando, para esclarecer y apreciar los hechos, sea conveniente que el juez examine por sí mismo algún lugar, objeto o persona. Puede darse esa necesidad tanto en fase declarativa como con ocasión del procedimiento de adopción de alguna medida cautelar.

1.2.5. Medios de reproducción del sonido o la imagen e instrumentos de archivo

Mediante la prueba de medios de reproducción del sonido e imagen el legislador da cabida a las películas, cintas de vídeo o medios de grabación; y por instrumentos de archivo, la ley se refiere a los disquetes flexibles y discos duros de ordenador, los *CDs* y *DVDs*, el correo electrónico, ficheros informatizados, o cualquier otro medio técnico de estas características que en el futuro pueda ser inventado.

¹⁰ Art 339 LEC: 2. El demandante o el demandado, aunque no se hallen en el caso del apartado anterior, también podrán solicitar en sus respectivos escritos iniciales que se proceda a la designación judicial de perito, si entienden conveniente o necesario para sus intereses la emisión de informe pericial. En tal caso, el tribunal procederá a la designación. Dicho dictamen será a costa de quien lo haya pedido, sin perjuicio de lo que pudiere acordarse en materia de costas.

4. En los casos señalados en los dos apartados anteriores, si las partes que solicitasen la designación de un perito por el tribunal estuviesen además de acuerdo en que el dictamen sea emitido por una determinada persona o entidad, así lo acordará el tribunal. Si no hubiese acuerdo de las partes, el perito será designado por el procedimiento establecido en el artículo 341.

5. El tribunal podrá, de oficio, designar perito cuando la pericia sea pertinente en procesos sobre declaración o impugnación de la filiación, paternidad y maternidad, sobre la capacidad de las personas o en procesos matrimoniales.

El procedimiento probatorio consiste en la aportación y posterior reproducción ante el tribunal de las imágenes y sonidos. Así, las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes (art. 382.1 primer inciso). A esta proposición, las partes pueden acompañar: la transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso (art 382.1 inciso final); así como los dictámenes y medios de prueba instrumentales que considere convenientes. Del mismo modo, la parte no proponente de esta prueba podrá, cuando cuestione la autenticidad y veracidad de lo reproducido, aportar dictámenes o medios de prueba que acrediten su postura (art. 382.2). Además, la documentación se presentará del modo más apropiado a la naturaleza del instrumento, bajo la fe pública del Letrado de la Administración de Justicia, quien, en su caso, adoptará medidas de custodia cuando resulten necesarias.

2. LA PRUEBA DIGITAL O ELECTRÓNICA

2.1. Introducción y concepto

Según Francesco CARNELUTTI¹¹, la prueba es la actividad de acreditación de la realidad de un hecho afirmado por las partes y que tiene relevancia jurídica para el objeto del proceso. La información que se presente ante el juez en formato digital empleará un “lenguaje binario a través de un sistema que transforma impulsos o estímulos eléctricos o fotosensibles y, por cuya descomposición y recomposición informática grabada en un formato electrónico, genera y almacena la información. Dicho lenguaje es un código ininteligible para aquellos que no son informáticos. La visualización del texto en pantalla es una traducción en lenguaje alfabético común, descodificado. De este modo, el archivo se conserva en un sistema binario. En

¹¹ Montero Aroca J, Gómez Colomer JL, Barona Vilar S, Calderón Cuadrado MP; *Derecho Jurisdiccional II Proceso Civil*, Tirant Lo Blanch; Valencia, 2014, p. 219.

cambio, el texto exteriorizado es fruto de la transformación de ese sistema binario en forma de escritura, con letras de nuestro alfabeto” (GARCÍA TORRES)¹².

La información en forma electrónica se produce y se almacena en instrumentos o dispositivos electrónicos. De aquí en adelante, emplearemos el concepto de dispositivo electrónico o digital para designar los sistemas informáticos y los aparatos tecnológicos. En este concepto incluiremos teléfonos móviles, ordenadores, tablets, pendrives, disco duros o DVD entre otros.

Concluiremos este apartado con una breve definición de la prueba digital en palabras de Carolina SANCHÍS CRESPO: la prueba digital o electrónica es aquella en la que toda la información que tiene valor probatorio para el proceso se encuentra o se transmite mediante un medio electrónico¹³.

La prueba electrónica ha sido introducida por la LEC 1/2000, sin embargo, ya había sido considerada e incluida por nuestra jurisprudencia con anterioridad¹⁴.

¹² García Torres, ML., *La tramitación electrónica de los procedimientos judiciales, según la ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil*, Revista Internacional de Estudios de Derecho Procesal y Arbitraje, www.riedpa.com, n° 3-2011, <http://www.riedpa.com/COMU/documentos/RIEDPA31102.pdf>

¹³ Sanchís Crespo, C., *La prueba en soporte electrónico. (Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia)*, Thomson Reuters Aranzadi, Navarra, 2012, p. 713.

¹⁴ Tribunal Supremo, Sala de lo Civil, sentencia núm. 4735/1999, de 12 de julio, fto. jco.6o: “Admisibilidad de las cintas magnetofónicas como medio de prueba sujeto a las normas de los documentos”.

Tribunal Supremo, Sala 1ª, sentencia núm. 4735/1999, de 12 de junio, fto. jco.7º: “Los medios de reproducción del sonido y la imagen se someten al régimen de la prueba documental, y de no ser reconocidos por la parte a quien perjudiquen han de ser sometidos a la correspondiente verificación o comprobación”.

Tribunal Constitucional, Sala Primera, sentencia núm. 190/1992, de 16 de noviembre de 1992, fto. jco.3o: “Admisibilidad de las cintas magnetofónicas: cautela derivada de posibilidad de manipulación, trucaje y distorsión y reconocimiento eficacia probatoria, particularmente cuando han sido incorporadas a las actuaciones, no han sido impugnadas en todo o parte y se dan por reproducidas en el acto del juicio”.

El artículo 24.2 CE recoge el derecho a hacer uso de todos los medios de prueba pertinentes y que consideremos necesarios. Ahora bien, en el mundo de hoy, en el que cada vez dependemos más de las nuevas tecnologías, se ha comenzado a producir la introducción en el mundo del derecho de nuevas fuentes y medios de prueba. Así, nace lo que hoy conocemos como prueba electrónica. Para fijar un concepto claro y conciso de éste es necesario recurrir a varios preceptos legales y esclarecer cuál es su naturaleza.

2.2. Naturaleza de la prueba digital o electrónica

La mayoría de la doctrina y la jurisprudencia coinciden en considerar la prueba electrónica como prueba documental por las semejanzas que guarda el soporte electrónico con el documento y por la idoneidad de su introducción en el proceso como tal.

En primer lugar, el artículo 26 CP define como documento todo *“soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica”*. Este es un concepto amplio ya que, junto al papel (medio tradicional) se da cabida a nuevos soportes tecnológicos e informáticos como videos, fotos, CDs, DVDs, disco duros, SMS o correos electrónicos. Además, el Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal (en lo sucesivo, LECrim) en su artículo 743 recoge un concepto de documento electrónico y dice así: *“el desarrollo de las sesiones del juicio oral se registrará en el soporte apto para la grabación y reproducción del sonido y de la imagen”*, enmarcando este concepto dentro del epígrafe *“Medios de registro de la sesión. El documento electrónico”*. Por último, cabe señalar que bajo los medios de prueba del artículo 299 LEC se menciona lo siguiente: *“los medios de reproducción de palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir las palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase...”*.

Por tanto, se puede concluir que un soporte es todo aquello que nos permite almacenar información y puede valerse para ello de cualquier material: papel, cinta de video,

pendrive o disco duro entre otros. Los datos obtenidos a partir de estos soportes serían la información que emplearíamos para probar los hechos afirmados durante el proceso, pudiendo estar dicha información recogida bien en una pagina web, un correo electrónico, una base de datos, una hoja de cálculo, un documento Word, un documento multimedia...¹⁵

Hay que tener en cuenta que el uso de estos medios e instrumentos consiste principalmente en adaptar los documentos clásicos a los soportes multimedia pero no dan cabida a Internet ni a las redes sociales. Internet, *“va más allá de ser un soporte documental representativo de una realidad fáctica, pues se concibe como un conjunto de miles de redes de ordenadores conectados entre sí que permite el acceso a una inmensa fuente de información práctica y disponible. (...). Por tanto, se debe considerar Internet como una fuente de prueba”*.¹⁶

La prueba electrónica en cuanto a prueba documental constará de: soporte material, puesto que es necesaria la desmaterialización del soporte y codificación del mensaje, es decir, hacer posible su lectura o traducción al lenguaje visual; contenido informativo, y, por último, relevancia jurídica, es decir, que se pueda a través de ellos acreditar hechos que sean jurídicamente relevantes en el proceso.

2.3. Normativa aplicable

En nuestro ordenamiento jurídico no existe una normativa específica para la prueba digital o electrónica, sino que se acude a las disposiciones generales aplicables a la prueba clásica o tradicional. A continuación, procederemos a un breve análisis de la normativa existente sobre esta materia en el ámbito internacional, comunitario y nacional.

¹⁵ Pérez Palaci E., *La prueba electrónica: Consideraciones*, Universitat Oberta de Catalunya, 3 de julio de 2014. (Disponible en <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf>) Consultada el 25/02/2017.

¹⁶ Alonso-Cuevillas Sayrol, J., *Internet y prueba civil*, Revista jurídica de Cataluña, año 2001, núm.4, p. 1079 y ss.

2.3.1. Ámbito internacional

En el marco de normativa internacional hay que destacar las Resoluciones 55/63 y 56/121 de la Asamblea General de la Organización de las Naciones Unidas (ONU en adelante). A través de ellas se pretende combatir el mal uso de las nuevas tecnologías y fomentar la cooperación entre Estados para coordinar los avances en investigación en el ámbito judicial.

Además, hay que destacar las Recomendaciones a Gobiernos nacionales y organizaciones internacionales en cuanto a la relevancia jurídica de los registros conservados en los dispositivos electrónicos, sobre todo ordenadores, teniendo en cuenta que fueron aprobadas en 1985 por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)¹⁷.

Por último, en 2005 tuvo lugar la Convención de la ONU sobre uso de las comunicaciones electrónicas en materia contractual internacional.

2.3.2. Ámbito de la Unión Europea

En el ámbito comunitario encontraríamos, en primer lugar, el Convenio Europeo de Derechos Humanos (CEDH en lo sucesivo). El art. 8.1 de dicho Convenio establece el derecho a la vida privada y familiar, el derecho a la inviolabilidad del domicilio y, en su apartado segundo restringe la intervención del Estado excepto “por causas de seguridad nacional o pública, bienestar económico nacional, defensa del orden, prevención de infracciones penal, o protección de los derechos y libertades de los demás”. El Convenio fue ratificado por España el 4 de octubre de 1979 (BOE de 10 de octubre de 1979).

En segundo lugar, nos encontramos con la Directiva 1999/93/CE que recoge un marco comunitario y único para la firma electrónica. Su art. 5 establece la necesidad de que

¹⁷ http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1985Recommendation.html
http://www.uncitral.org/pdf/spanish/publications/sales_publications/UNCITRAL-s.pdf

los Estados miembros admitan en un procedimiento judicial la firma electrónica como prueba.

También merece la pena mencionar el Programa sobre Cooperación Policial y Judicial en materia penal (AGIS) para favorecer, sobre todo en materia penal pero extendiéndolo a todos los ámbitos, la cooperación contra delitos de carácter telemático.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Tendrá especial relevancia en cuanto a la licitud de la obtención de la prueba digital.

Por último, la normativa más reciente en relación con la prueba digital es el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos. Su objeto es la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos. El Reglamento deroga la anterior Directiva de 1995 que se había quedado obsoleta y da paso a un nuevo marco normativo, otorgando un mayor grado de control a los ciudadanos sobre su información privada e imponiendo cambios radicales para las empresas, que deben empezar a adaptar sus protocolos y estructuras a la nueva regulación.

2.3.3. Ámbito nacional

Siendo la LEC nuestra fundamental referencia durante este trabajo, es preciso mencionar la existencia de otros textos legales de los que nos serviremos a lo largo de este análisis.

La Ley 59/2003, de 19 de diciembre, de Firma electrónica define en su art. 3.1 la firma electrónica como el conjunto de datos que, en forma electrónica, pueden servir para la identificación del firmante. A continuación, proporciona una definición de documento electrónico refiriéndose a éste como “*aquel que se redacta en un soporte electrónico y que incorpora datos firmados electrónicamente, pudiendo ser soporte*

de documentos públicos y privados, que tendrán la eficacia que se les otorgue la legislación aplicable”, remite, por tanto, a la normativa procesal civil. Por último, es muy relevante el art. 3.8 de esta Ley puesto que da la categoría de prueba documental a los datos firmados electrónicamente. Además, señala el proceso a seguir en caso de impugnación de la autenticidad de la firma electrónica.

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y redes de comunicaciones. El art. 3 enumera los datos que serán necesarios para poder identificar el origen y destino de una comunicación.

La Ley 34/2002, de 11 de julio de Sociedad de Servicios de la Información, que es relevante en cuanto que admite como prueba documental el “*sopORTE electrónico en que conste un contrato celebrado por vía electrónica*” (art. 24).

No podemos dejar sin mención el articulado de la LEC que será aplicable a la prueba digital. El Libro II, Capítulo V (arts. 281 a 386), especial mención al a los arts. 382-384 que recogen los denominados nuevos medios de prueba (hay que decir que la LEC no menciona en concreto la prueba digital o electrónica, lo que nos lleva a aplicar analógicamente lo dispuesto para los documentos privados empleando esos nuevos medios de prueba). En cuanto a los derechos fundamentales, especialmente relevantes en cuanto a su respeto y no vulneración en la obtención de la prueba digital, analizaremos en apartados sucesivos, la importancia de los tres primeros apartados del art. 18 CE.

2.4. Principales medios de prueba digital

En principio, los medios de prueba que prevé la LEC en su art. 299 son adecuados para la incorporación al proceso de la prueba digital o electrónica. Éstos serán objeto de un análisis más profundo en el punto 4.3 del presente trabajo, en el cual se trata la incorporación al proceso de la prueba digital. Sin embargo, a continuación destacaremos lo más relevante de cada uno de ellos sin entrar en detalle. Aunque, como ya se indica, los medios de la prueba digital no presentan especial complejidad debido a que no hay apenas diferencias con los medios de prueba tradicionales, el

propósito de este breve análisis radica en proporcionar un mejor entendimiento del apartado siguiente: las fuentes de prueba digital. Al contrario que en los medios de prueba digital, las fuentes sí presentan mayor especialidad y merecen una explicación más extensa, que no es del todo posible sin subrayar cuáles son los medios de prueba pertinentes en este ámbito.

El primer medio de prueba será la prueba documental en soporte papel. Esta prueba consistirá simplemente en la impresión en formato papel de la información de interés. Se aplicará el régimen de la prueba documental tradicional. En caso de impugnación, la parte que aportó la prueba podrá servirse de otros medios, normalmente la prueba pericial, para tratar de acreditar la veracidad de lo aportado. Si se aportara conjuntamente acta Notarial, estaríamos ante la prueba de documento público.

En segundo lugar, nos encontramos con la prueba de documento electrónico que consiste, básicamente, en la incorporación de la información a un soporte electrónico. En este caso, aplicaríamos el régimen jurídico de la prueba de instrumentos electrónicos (art. 283 y 384 LEC). Así, lo que realmente se aporta al proceso es el soporte en el se incluye la información. Los más habituales son un pen-drive, un CD o un DVD.

Siendo estos los medios de prueba digital más frecuentes, no podemos dejar de mencionar, la prueba pericial. La prueba pericial juega un papel fundamental en la prueba digital. Puede aportarse como prueba independiente, o como prueba complementaria a otra. Además, puede aportarse la prueba pericial con la finalidad de probar y acreditar la no manipulación de lo aportado.¹⁸ Dedicaremos un apartado en concreto para el análisis de este medio de prueba ya que responde a uno de los principales objetos de este trabajo: la verificación de la prueba digital.

¹⁸ Vegas Torres, J., *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*, Universidad Rey Juan Carlos, Cátedra de Investigación Financiera y Forense KPMG-URJC, Madrid, 2011, p. 135.

2.5. Principales fuentes de prueba digital

2.5.1. Correo electrónico

A través de un correo electrónico o e-mail se transmite tanto texto como imágenes o sonidos. Su aportación al proceso como prueba digital se enmarca dentro del art. 384 LEC. Es una prueba que hoy en día se admite en un proceso sin ningún inconveniente.

Hay determinados sistemas de e-mails que almacenan en el servidor el contenido de los mensajes remitidos y recibidos. Incluso hay casos en los que, una vez que el usuario los ha eliminado de su bandeja de entrada, el servidor guarda una copia de respaldo. Hay dos sistemas de recuperación de mensajes desde los servidores: Post Office Protocol y Internet Message Access Protocol. Sin embargo, a pesar de que el servidor haya guardado una copia del mensaje, es realmente difícil acceder a ella para recuperar el contenido. Por ello, el contenido de los correos electrónicos como prueba se suele realizar a través del acceso a los datos contenidos en los dispositivos electrónicos empleados por emisor y receptor de la comunicación (prueba documental).

Lo más corriente es la obtención e incorporación al proceso de la información contenida en los dispositivos usados en la comunicación. El acceso al dispositivo afecta a la intimidad personal y por ello siempre debe hacerse de manera lícita. ¿Cómo se puede aportar el contenido de un e-mail en forma de prueba al proceso? El correo electrónico se encuentra dentro de un dispositivo y, por tanto, necesita un sistema operativo. Por esta razón, la manera más sencilla de aportarlo al proceso sería a través de una copia impresa, es decir, como documento en soporte papel. En este caso sería documento privado aunque siempre se podrá elevar a documento público cumpliendo con las formalidades necesarias y el acta de presencia notarial. También es posible su aportación como documento electrónico. En estos casos lo que se incorpora al proceso es el soporte en sí, es decir, un pendrive, un DVD y otros medios que permiten el almacenamiento de datos. Hoy en día, es muy frecuente la firma digital en los correos electrónicos. Esto facilita la verificación y autenticidad del contenido y autoria de éste puesto que estas firmas se instalan mediante diferentes

tecnologías de firma electrónica. Algunos ejemplos son las tecnologías como S/MIME usada por Microsoft, o DKIM usada por Google o Yahoo.

Hay ocasiones, normalmente ante la impugnación de la parte contraria, en las que es preciso un informe de un perito. En estos casos se deberá “aportar el código fuente que permite acreditar:

- la identidad de la dirección de correo del emisor del mensaje
- la identidad del equipo desde el que se emite, lo que conocemos como dirección de IP
- la identidad del servidor del correo saliente
- la identidad del servidor del correo entrante, y
- la fecha y hora de su envío y recepción”¹⁹

Si la parte contraria impugnara el correo electrónico como prueba no se le privaría a éste de eficacia. Simplemente, la parte que lo aportó deberá ocuparse de demostrar su veracidad y autenticidad. En caso de que no se consiguiera probar su autenticidad pero tampoco su inautenticidad, el órgano judicial podrá valorarlo conforme a la sana crítica y otorgarle eficacia cuando existan en el proceso otros elementos de prueba susceptibles de ser valorados con el correo y que corroboren lo que éste intenta probar.

2.5.2. Páginas web

Una página web es, según Xavier ABEL LLUCH²⁰, un tipo de documento informático accesible mediante Internet y la identificación de un enlace. Las webs funcionan con unos códigos instalados y entendidos por los navegadores y están colocadas en servidores a los que se accede mediante Internet. A través de una página web se ofrece a todos los usuarios, prácticamente, cualquier tipo de información.

Al igual que lo hacía el correo electrónico, las páginas web, a la hora de acceder al proceso como prueba, se enmarcan en el art. 384 LEC. Sin embargo, a diferencia de

¹⁹ Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p. 454.

²⁰ Abel Lluch, X., *Prueba electrónica*, Ginés Castellet. N., *Serie de estudios prácticos sobre los medios de prueba*, ESADE, Bosch Editor, 2011, p. 217 y ss.

éste, no sirve para el intercambio de información entre personas sino para la difusión de ésta.

La página web puede acceder al proceso en forma de prueba como prueba documental no solo como documento privado sino también como documento público. Si fuera como documento privado estaríamos ante la impresión del contenido de la página web y su presentación al órgano judicial. Si fuera como documento público, una vez más hay que añadir el acta de protocolización del notario y, en algunos casos, el acta de presencia para que el notario navegue por Internet. Además, las páginas web pueden incorporarse al proceso mediante el interrogatorio de las partes o de testigos, o también, mediante la prueba pericial con el informe del perito informático²¹.

Como sucedía con los e-mails, el tribunal admitirá como prueba la impresión de la página web aunque no vaya acompañada de un informe pericial. Ahora bien, en caso de impugnación la carga de la prueba corresponde a la parte perjudicada por el contenido de la web²².

2.5.3. Mensajes de teléfono móvil (SMS)

El SMS (short message service) es un servicio para aquellas personas titulares de un teléfono móvil que posibilita el intercambio de mensajes de texto cortos entre móviles. Los SMS son una modalidad de documentos informáticos que se enmarcan tanto en el 384 LEC (archivo de datos) como en el 382 LEC (grabación, fotografías, descargas de música...) y además, podemos decir que se trata de una comunicación en canal cerrado²³.

Los mensajes de teléfono móvil se pueden aportar sin inconvenientes como prueba a un proceso judicial. Sin embargo, presentan dos problemas difíciles de subsanar: por

²¹ Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p. 455.

²³ Bueno Aguado, CM., *Los SMS a efecto de notificación*, Revista General de Derecho Procesal, núm. 37, 2015, Iustel.

un lado, la fácil manipulación y, por otro, la dificultad en demostrar la autoría²⁴. Cuando se aporta un mensaje de texto como prueba, la prueba plena abarca tres extremos: quien remite el mensaje mediante un terminal de telefonía móvil, quien lo recibe a través de otro terminal y, la integridad y autenticidad del mensaje²⁵.

El destinatario suele aportar al proceso el contenido del SMS que ha recibido mediante distintos medios de prueba (como ocurría en el correo electrónico, serían aceptables los documentos privados, públicos o electrónicos). Su identificación no suele dar lugar a excesivas complicaciones. El principal problema es, como ya hemos mencionado, demostrar la autoría. Lo primero que habría que hacer sería identificar el dispositivo en concreto mediante su código identificador (IMEI), y a continuación, determinar quién remitió ese mensaje de texto. El otro problema que enunciábamos era el de la fácil manipulación de los SMS y, por ende, la dificultad de demostrar la autenticidad y veracidad de los mismos. Hoy en día se recurre a los llamados Terceros de Confianza o Prestadores de Servicios de Confianza para acreditar la realización de una comunicación en formato electrónico como es el caso de los mensajes de texto²⁶.

2.5.4. WhatsApp y otros medios de mensajería instantánea

“La aplicación WhatsApp es la que ha conseguido más popularidad y se ha convertido casi en el estándar de la mensajería, contando con más de 6.000 millones de usuarios en todo el mundo”. Así comenzaba el diario ABC su artículo sobre “Las mejores aplicaciones de mensajería instantánea” el 11 de noviembre de 2011. Y es que, poco a poco, los SMS y MMS han ido dejando paso a las aplicaciones de mensajería instantánea como WhatsApp, Line o Telegram.

Las características básicas de estos sistemas de mensajería instantánea son, entre otras, la habilitación de las comunicaciones mediante aplicaciones y entre usuarios, y su disponibilidad para múltiples plataformas como IOS (iPhone), Android, Windows

²⁵ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 178.

²⁶ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 179.

Phone o Blackberry OS. Además, la información que los usuarios intercambian no se conserva en ningún servidor que no sean los propios dispositivos desde los cuales se emiten o reciben los mensajes. Es más, existe la garantía de que se usan protocolos de seguridad para garantizar el cifrado de la información²⁷.

Lo expuesto previamente sobre los mensajes ed teléfono móvil es perfectamente aplicable a estos medios sin embargo, la problemática que se presentaba cobra ahora mucha más importancia. Cualquiera que tenga unos mínimos conocimientos informáticos puede manipular los mensajes. Por esta razón, su admisión como prueba se hace con grandes reservas y mucha precaución.

El peligro que nace de la fácil manipulación a la que esta prueba está sometida, ha sido observada en reiteradas resoluciones por la jurisprudencia. El Tribunal Supremo ha señalado la necesidad de abordar la prueba de una comunicación bidireccional, como la de WhatsApp, con gran cautela. Como señala también Javier RUBIO ALAMILLO en su blog *‘Peritaje informático de conversaciones de WhatsApp o aplicaciones similares’*, el riesgo de manipulación de estas pruebas es elevado ya que *“el usuario puede eliminar la coversación sin dejar rastro de ella en su móvil, aunque un examen pericial forense del teléfono móvil podría recuperarla mediante un procedimiento de complejidad elevada; o mensajes que realmente no han sido enviados pueden ser ‘colocados’ como remitidos. [...] En definitiva, y como afirma la STS 754/2015, de 27 de noviembre, “las posibilidades de manipulación son muy variadas y el órgano jurisdiccional tiene que ponerse en guardia con todas las cautelas que sean recomendables ante la posibilidad de una supercherías” [...]”*.

¿Cómo se pueden incorporar al proceso estos mensajes? El contenido de los mensajes intercambiados en WhatsApp (o cualquiera de los otros sistemas de mensajería instantánea) pueden acceder al proceso de maneras distintas. En primer lugar, se puede aportar el propio dispositivo, es decir, el teléfono móvil o ‘smartphone’ en el que encontremos los mensajes recibidos y enviados. Ésta suele ser la alternativa más usual. Además, se puede aportar una transcripción escrita de la conversación en

²⁷ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 180.

cuestión solicitando el cotejo por el Letrado de la Administración de Justicia. Si se considera necesario, se puede aportar conjuntamente con un acta notarial sobre el contenido de la concreta conversación de WhatsApp que se pretende probar. Hay ocasiones en las que se procede a la entrega del dispositivo para que sea objeto de reconocimiento judicial, a veces, incluso en el propio juicio. Por supuesto, como en los casos anteriores, los contenidos de esas conversaciones pueden ser objeto de prueba testifical²⁸.

En los casos expuestos *supra* la prueba es válida sin perjuicio de la valoración de la eficacia probatoria que el órgano judicial le otorgue en su valoración. Normalmente, en ausencia de impugnación, el juez o tribunal le otorgará plena eficacia probatoria. En caso contrario, si la otra parte impugna la prueba alegando que manipulación o falsedad, el órgano judicial valorará los argumentos de impugnación y tendrá en cuenta otros medios de prueba. En este punto, cobraría especial importancia la prueba pericial²⁹.

Es muy útil la referencia a la STS 300/2015, de 19 de mayo³⁰, en la cual el tribunal se pronuncia sobre la validez que los mensajes de estos medios o sistemas de comunicación pueden tener como prueba y realza la necesidad de realizar una prueba pericial. De hecho, el tribunal sentenció que, parafraseando a LEFEBVRE “*cuando las conversaciones de las redes sociales se ponen en duda y se aportan a la causa archivos impresos, se desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria*”. El Supremo insistió en la necesidad de realizar una prueba pericial en estos casos, calificándola de indispensable. Con ésta se conseguiría la identificación del verdadero origen de la comunicación, la identidad de los interlocutores y la información contenida de manera íntegra. En cualquier caso, el tribunal señaló que las pruebas de este tipo deben ser siempre admitidas en el proceso con todas las cautelas ya que la posibilidad de manipulación es altísima.

²⁸ Alonso-Cuevillas, J., *Internet y prueba civil*, Revista Jurídica de Catalunya, Vol. 100, núm 4, 2001, p. 1082 y ss.

²⁹ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p.182-187.

³⁰ Tribunal Supremo (Sala Segunda), Sentencia núm. 300/2015, de 19 de mayo.

El punto de vista de que la carga de la prueba recae en quien aporta esas pruebas ha sido puntualizado por parte de la doctrina en los últimos tiempos; y es que los denominados pantallazos de los mensajes que se envían por cualquier medio de mensajería instantánea o por redes sociales (Facebook, Twitter, WhatsApp, Telegram, Instagram, Skype)³¹ se aportan al proceso en forma de documentos privados y, por tanto, cuando son impugnados pero no se consigue demostrar ni su validez ni tampoco su falsedad, se podrán tener en cuenta junto con otros elementos del proceso³².

A este respecto y para finalizar este subapartado, es de interés citar la STS 754/2015, de 27 de noviembre³³, cuyo objeto es la aportación de ‘pantallazos’ al proceso como prueba. Éstos se obtuvieron del teléfono móvil de la víctima y fueron tomados en consideración por el tribunal gracias, en parte, a que su veracidad y autenticidad quedaron acreditadas por el reconocimiento que hizo el acusado a través de su escrito de defensa.

Por último, una breve mención a la cuestión de la autoría del mensaje y de la titularidad de la línea desde la que se envía o en la que se recibe. La razón nos lleva a pensar que es el titular de la línea el que lleva a cabo la comunicación en cuestión y, por tanto, es deber de quien lo niega acreditar aquellos hechos que así lo demuestren.

2.5.5. Redes sociales

Una red social como Facebook o una página web como fuentes de prueba se deben aportar al proceso mediante los medios previstos en el art. 299 LEC, no solo en su apartado primero, el cual contiene los medios de prueba tradicionales, sino también en su apartado segundo en el que se enumeran los medios de reproducción audiovisuales

³² Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p.455, 456.

³³ Tribunal Supremo (Sala Segunda), Sentencia núm. 754/2015 de 27 de noviembre.

y los instrumentos informáticos³⁴.

Las distintas informaciones que “colgamos” en las redes sociales, en los perfiles abiertos, pueden ser relevantes en cuanto a elementos probatorios de distintos hechos en un proceso judicial. Realmente, cuando los usuarios “cuelgan” esas informaciones en los perfiles de las redes sociales, se entiende que no esperan ningún tipo de privacidad por lo que rara vez nos encontraremos con vulneraciones a derechos fundamentales como el derecho a la intimidad. Poco a poco, conforme los usuarios van actuando ‘on-line’, van dejando huellas en blogs, redes sociales, buscadores, foros. Podríamos decir que va creando su propia identidad ‘on-line’. Siguiendo la tesis de Xavier ABEL LLUCH³⁵, el análisis de esos rastros digitales en las redes “puede aportar pruebas o indicios muy valiosos no solamente de hechos ocurridos en dichas redes, sino también de hechos cometidos en el mundo físico”.

Un e-mail o una página web pueden acceder al proceso mediante las pruebas personales, entre las que se encuentran el interrogatorio de las partes, de testigos y de peritos. Así, en la declaración, el declarante puede decir que ha recibido un determinado e-mail, puede hablar del contenido de un sitio web o puede hablar de comentarios y posts publicados en Facebook o Instagram. Incluso alguien podría declarar que fue testigo de cómo un tercero llevaba a cabo alguna de estas acciones desde su ordenador.

A este respecto el testimonio del perito y su dictamen resultan cruciales porque, al aportar sus conocimientos informáticos especializados pueden explicar el proceso de remisión y envío de esas informaciones³⁶.

Los contenidos mencionados en el apartado anterior (correos electrónicos, informaciones de un sitio web, posts o comentarios en redes sociales como Facebook o Instagram) pueden acceder al proceso en forma de documentos privados. Lo más

³⁴ Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, Bosch Editor, 2011, p. 275.

³⁵ Abel Lluch, X., *Prueba electrónica*, Ginés Castellet, N., *Serie de estudios prácticos sobre los medios de prueba*, ESADE, Bosch Editor, 2011, p. 201.

³⁶ Queral Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, Bosch Editor, p. 276

fácil en este contexto sería su impresión, la impresión de los pantallazos (fotos a la pantalla) realizados desde el dispositivo móvil o el ordenador.

Su eficacia probatoria dependerá de la impugnación, o ausencia de ella, por la parte contraria (art. 326 LEC). En caso de impugnación siempre es de gran importancia aportar una prueba pericial informática para intentar acreditar su autenticidad.

Además, el contenido de un e-mail o una página web podrá incorporarse al proceso mediante un documento público. En estos casos se aportaría un acta de protocolización notarial. En ésta el Notario protocoliza en acta la impresión privada que ha hecho la parte del contenido concreto de Internet que quiere incorporar como prueba. Es necesario precisar que el Notario da fe de que esa persona le entregó unos documentos, pero no da fe de la existencia de esas informaciones en la determinada página web o red social. Para subsanar este efecto, se puede aportar un acta de presencia que requerirá la presencia del notario para que navegue por Internet y busque la información concreta. De este modo se conseguiría que la fe notarial se extendiera a los contenidos determinados que se quieren probar.

El dictamen pericial serviría como auxiliar a la prueba digital aportada. Sobre todo, es de gran utilidad cuando la parte contraria impugna la prueba documental aportada. Por otro lado, como ya se ha explicado más extensamente, se puede aportar una prueba pericial independiente para acreditar un contenido de Internet, de e-mail o de publicaciones o mensajes en una red social.

Otro medio de prueba útil a este respecto es el reconocimiento judicial. Consiste, a grandes rasgos, en el examen por el tribunal de un objeto, lugar o persona (art 353 LEC). En este caso, consistiría en el reconocimiento de la red social o del sitio web como un reconocimiento de lugar virtual, aunque también se puede realizar el reconocimiento de un dispositivo, como un móvil o un ordenador. Con este medio de prueba se permite que el propio juez, el tribunal en su caso, acceda de modo directo al contenido de la red mediante la cibernavegación³⁷.

³⁷ Queral Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, 2011, Bosch Editor, p. 277-279.

Es necesario proponer la cibernavegación y concretar la página web o red social en concreto a la que se quiere acceder. Además, será necesario especificar si existe en la sede judicial un ordenador habilitado para su práctica en presencia de las partes. Lo más importante del reconocimiento judicial es el examen llevado a cabo directa y personalmente por el juez.

El reconocimiento judicial puede practicarse junto con la prueba pericial informática o con los interrogatorios como establece la LEC en sus arts. 356 y 357. Cuando se lleve a cabo la práctica de esta prueba, se levantará acta por el letrado de la administración de justicia y se dejará constancia de todo aquello que haya sido objeto del reconocimiento mediante grabaciones y vídeos (art. 359 LEC).

La mayor problemática que surge en el marco del reconocimiento judicial es el constante cambio que sufren los contenidos de Internet y de las redes sociales y la facilidad que hay para borrar y eliminar cualquier rastro de información. Por tanto, cobra especial relevancia la práctica de la prueba anticipada. El requisito a cumplir para poder llevarla a cabo es el temor fundado de que determinados contenidos pueden desaparecer y que, por tanto, en el momento de llevar a cabo el reconocimiento judicial puedan no encontrarse y ser imposible su acceso. Una solución sería la grabación o impresión de esos contenidos en un soporte que se pueda aportar al proceso y aportar junto a él el acta notarial de presencia. También se podría pedir un dictamen pericial y aportarlo junto con dicho soporte.

Finalmente, una breve mención a los medios audiovisuales e instrumentos informáticos tales como pen-drive, DVDs, CDs o tarjetas de memoria. En éstos se podrá almacenar cualquier contenido de las redes sociales o páginas web. La parte las aportará del mismo modo y con los mismos requisitos a cumplir que en los documentos privados. Resulta útil aportar junto con ellos dictámenes periciales que puedan ayudar en su valoración y verificación³⁸.

³⁸ Queral Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, Bosch Editor, 2011, p. 279.

3. LA PRUEBA DIGITAL O ELECTRÓNICA EN EL PROCESO. ESPECIAL REFERENCIA AL PROCESO CIVIL

Llegados a este punto, explicaremos de manera breve las fases por las que atraviesa la prueba digital o electrónica en el proceso: la **obtención** de la información, la **incorporación** al proceso y, por último, la **valoración**. Éstas serán objeto de análisis en los tres apartados que siguen. Sin embargo, antes de adentrarnos en dicho análisis es preciso hablar del momento de proposición de la prueba electrónica o digital.

El análisis que sigue se centra en el proceso civil, si bien hay que añadir que el régimen común a la prueba digital o electrónica se fundamenta en la normativa propia de dicho proceso. Esto se debe principalmente a dos razones: la LEC es el único ordenamiento procesal que se refiere a ella, y, además, su regulación se aplica de forma subsidiaria en el resto de jurisdicciones por el art. 4 LEC.

3.1. Proposición de la prueba digital y momento de aportación

La LEC equipara el momento de aportación de la prueba electrónica al de la prueba documental (arts. 382-384 LEC) de forma que debe aportarse con carácter general con la demanda o la contestación a la demanda. El artículo 265.2 LEC que prevé que “*con la demanda, la contestación o, en su caso, al comparecer a la vista de juicio verbal, habrán de presentarse: los medios o instrumentos a que se refiere el apartado 2 del art. 299, si en ellos se fundaran las pretensiones de las partes*”. Como consecuencia, hay que determinar, igual que ocurre con los clásicos documentos, si se trata de medios electrónicos fundamentales o no, pues sólo cuando sean fundamentales será obligatoria su aportación con la demanda o la contestación³⁹.

³⁹ SAP de Barcelona, secc. 15a, Sentencia núm. 259/2008, de 2 de julio: “*Siendo así, el momento para su aportación era la audiencia previa; si no se aportaron entonces, fue porque FÓRMULA ONE LICENSING no había acudido todavía a las webs que le interesaban, no pudiendo luego justificar que no se podían obtener con anterioridad a ese momento, o que no se tenía conocimiento de ellas. Las impresiones aportadas muestran que la fecha de acceso a la web fue en abril de 2007, poco antes de su presentación en el Juzgado, por lo que, estando disponible internet desde antes del comienzo de la litis, no se acompañan documentos desconocidos o que la parte no podía obtener, sino que se hace uso de un medio probatorio perfectamente accesible una vez precluido claramente el momento para ello [...]*”.

La LEC prevé, sin embargo, unas excepciones que permiten la aportación posterior posibilitando que el actor presente los medios e instrumentos electrónicos o digitales relativos al fondo del asunto en tres casos: en primer lugar, aquellos casos en los que los documentos sean de fecha posterior a la demanda o a la contestación y que hubiera sido imposible su producción en momentos anteriores; en segundo lugar, aquellos supuestos en los que la parte que presenta los medios de prueba no hubiera tenido constancia de su existencia y lo justifique; y, por último, en aquellas situaciones en las que no fuera posible obtener esos medios anteriormente. Sin embargo, la fecha de un documento de este tipo es fácil de manipular y por ello debe tomarse especial precaución a la hora de admitir un documento electrónico alegando que sea de fecha posterior a la demanda o contestación (pudiendo fácilmente ser de un momento anterior pero con una fecha alterada)⁴⁰ (art. 270.1.1 LEC).

3.2. Obtención de la prueba digital

La fase de obtención de la prueba consiste, primordialmente en obtener los datos o la información. Son las partes las que deben llevar a cabo esta labor, a diferencia del proceso penal en el que también puede desarrollar esta tarea la autoridad pública competente. Se trata de conseguir el acceso a la información relevante contenida o almacenada en los dispositivos electrónicos o que se hayan transmitido de manera digital mediante correos, Internet o chats de mensajería instantánea entre otros.

Dado que el objeto de este trabajo es el análisis de la prueba digital en el proceso civil, solo explicaremos la obtención de la prueba por la parte procesal, dejando a un lado su obtención por la autoridad pública competente en los procesos penales.

Como ya sabemos, la información que las partes pretenden llevar al proceso pueden presentarse de dos maneras: bien encontrándose en un dispositivo electrónico, o bien, habiendo sido transmitida por vía digital.

3.2.1. Información contenida en un dispositivo electrónico

⁴⁰ Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p. 450.

En este caso, el problema al que las partes se enfrentarían sería la titularidad del dispositivo. Es decir, la información y los datos de interés de cara al proceso civil pueden encontrarse en un dispositivo propio o en uno ajeno.

En caso de que el dispositivo sea propio, es decir, la parte interesada sea titular de dicho dispositivo el único problema al que nos enfrentaremos será la forma de incorporación al proceso manteniendo la autenticidad y la integridad de la información. Y, por supuesto, ser capaces de acreditar dicha autenticidad e integridad. En cambio, en caso de que la información de interés se encuentre en un dispositivo ajeno, pueden ser datos aportados por orden judicial o, más complejo aún, pueden ser datos obtenidos infringiendo derechos fundamentales. En este último caso la prueba sería ilícita. Más adelante, analizaremos la ilicitud de la prueba digital y sobre todo, los derechos fundamentales susceptibles de ser infringidos en estos supuestos.

3.2.2. Información transmitida por vía digital

Si la información se hubiera transmitido por redes de comunicación digitales también encontraremos dos posibilidades: que uno de los partícipes en la comunicación acceda a la información en ella transmitida para su posterior incorporación como prueba procesal, o bien, que la información se halle en una red de comunicación como Internet (no hay un proceso de comunicación entre partes, nos referimos, por ejemplo, a informaciones en páginas web).

En ambas situaciones, ¿cómo se presentan las informaciones obtenidas en forma de prueba? Es decir, ¿cómo se lleva a cabo la incorporación al proceso?

3.3. Incorporación al proceso de la prueba digital

La incorporación al proceso es la segunda fase de la prueba digital o electrónica. Y consiste en, una vez obtenida la información, hacer posible su acceso al proceso.

A grandes rasgos y en base al artículo 11.1 LOPJ⁴¹ ya citado previamente, la admisión de pruebas electrónicas en el proceso está condicionada a un juicio de licitud en el que se valora y verifica que éstas se hayan obtenido sin violar derechos fundamentales. Además, su uso en el proceso dependerá de su autenticidad e integridad, es decir, no se pueden haber manipulado y debe haberse conservado todo el contenido.

La información debe ser relevante para acreditar los hechos que las partes intentan probar. Tienen que ser relevantes jurídicamente. Para que la información obtenida acceda al proceso se deben cumplir los tres requisitos siguientes. En primer lugar, la información debe ser necesaria y útil. Es decir, debe ser relevante de cara a acreditar los hechos objeto del proceso y debe existir una relación entre esa información y los hechos controvertidos. En segundo lugar, debe ser lícita. Debe ser lícita no sólo en la fase de obtención pre-procesal, en la cual no se puede dar ningún tipo de infracción de derechos fundamentales; sino también en la fase de práctica del medio probatorio. Por último, siempre deben cumplirse los requisitos exigidos por la legalidad. A estos efectos, recurriremos al artículo 230.2 LOPJ⁴² que dice así: *“Los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales”*. Más concretamente, la información debe acceder al proceso mediante un medio probatorio admitido por la ley y, además, se debe respetar el procedimiento establecido para ese concreto medio de prueba.⁴³

⁴² Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. BOE (2 de Julio de 1985)

⁴³ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 48 – 76

3.3.1. ¿A través de qué medios de prueba se puede incorporar al proceso la prueba digital?

La información contenida en un dispositivo electrónico o obtenida a través de una red de comunicación digital debe incorporarse al proceso en un soporte determinado. Los datos pueden tener acceso al proceso por los medios de prueba tradicionales como pueden ser los interrogatorios, las pruebas periciales, las pruebas testificales o el reconocimiento judicial. Sin embargo, lo más común es que se presenten como documentos en soporte papel o como documentos electrónicos⁴⁴. Ahora sí, procederemos a un examen exhaustivo de los concretos medios de prueba digital.

a) Como documento en soporte papel

En estos casos, el contenido de la prueba electrónica se imprime en soporte papel y se incorpora el documento impreso⁴⁵. Es la manera que más se emplea en nuestro derecho pues se aplica la normativa y requisitos legalmente previstos para la prueba documental tradicional. En este caso, no es necesario identificar el hardware o el equipo del que procede el documento electrónico. Esto será necesario cuando la parte contraria impugne el documento. En ese escenario, habrá que practicar las pruebas necesarias para acreditar su autenticidad. Cobrará mucha importancia la prueba pericial informática de la que hablaremos más *in extenso* más adelante. Posteriormente analizaremos cómo se puede probar la autenticidad y veracidad del documento y, sobre todo, de la información que éste contiene. Sin embargo, hasta que llegemos a tal análisis nos limitaremos a decir que mientras la parte contraria no impugne el documento, éste tendrá una mayor fuerza probatoria de cara al juez o tribunal.⁴⁶ Ahora bien, dada la gran facilidad con la que se puede hacer desaparecer

⁴⁴ Queral Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, Bosch Editor, 2011.

⁴⁵ SAP Santa Cruz de Tenerife, secc. 4a, de 18 de noviembre de 2009, fto. jco.2o (JUR 2010/77692). “La aportación de una copia del documento multimedia mediante su transcripción en soporte papel permite una mayor accesibilidad al documento”.

⁴⁶ Artículo 326 LEC: *Fuerza probatoria de los documentos privados*
1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.
2. Cuando se impugne la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y

un documento del hardware de un ordenador y borrar cualquier rastro, suele resultar más útil identificar el servidor del que emana la información. GARCÍA PAREDES habla, a este respecto, de la necesidad de “indicar el archivo auténtico y original con el que puede ser cotejado cuando se aporte el hecho informático o electrónico en papel mediante una impresión como documento auxiliar o de referencia”.

Cabe citar a este respecto una STS 300/2015 de 19 de mayo⁴⁷, en la cual se recurre una sentencia condenatoria por abusos sexuales. El Tribunal Supremo admite el recurso de casación presentado por quien fue condenado previamente por la Audiencia Provincial de Valladolid por un delito de abusos sexuales. Entre las pruebas que se aportan en casación, se encuentran unas conversaciones mantenidas entre el condenado y la demandante por el servicio de mensajería instantánea de la red social ‘Tuenti’. Las pruebas se aportaron como ‘pantallazos’ de las conversaciones y sirvieron para disminuir la credibilidad de la demandante y poner en duda los hechos alegados. La prueba se presentó como prueba documental al imprimir esos

pertinente al efecto.

Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.

Artículo 319 LEC: Fuerza probatoria de los documentos públicos

1. Con los requisitos y en los casos de los artículos siguientes, los documentos públicos comprendidos en los números 1.º a 6.º del artículo 317 harán prueba plena del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan en ella.

2. La fuerza probatoria de los documentos administrativos no comprendidos en los números 5.º y 6.º del artículo 317 a los que las leyes otorguen el carácter de públicos, será la que establezcan las leyes que les reconozca tal carácter. En defecto de disposición expresa en tales leyes, los hechos, actos o estados de cosas que consten en los referidos documentos se tendrán por ciertos, a los efectos de la sentencia que se dicte, salvo que otros medios de prueba desvirtúen la certeza de lo documentado.

3. En materia de usura, los tribunales resolverán en cada caso formando libremente su convicción sin vinculación a lo establecido en el apartado primero de este artículo.

Artículo 320 LEC: Impugnación del valor probatorio del documento público. Cotejo o comprobación

1. Si se impugnase la autenticidad de un documento público, para que pueda hacer prueba plena se procederá de la forma siguiente:

1.º Las copias, certificaciones o testimonios fehacientes se cotejarán o comprobarán con los originales, dondequiera que se encuentren, ya se hayan presentado en soporte papel o electrónico, informático o digital. 2.º Las pólizas intervenidas por corredor de comercio colegiado se comprobarán con los asientos de su Libro Registro.

⁴⁷ Tribunal Supremo (Sala de lo Penal), Sentencia núm. 300/2015, de 19 de mayo.

pantallazos que mostraban las conversaciones, objeto de la prueba. Sin embargo, el caso tiene relevancia a efectos de la incorporación de la prueba digital al proceso puesto que *“incurre en la causa de inadmisión -ahora desestimación- prevista en el art. 884.4 de la LECrim, en la medida en que se señalan como documentos lo que no tiene tal carácter a efectos casacionales. Las conversaciones incorporadas a la causa mediante "pantallazos" obtenidos a partir del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales. Se trata de una prueba personal que ha sido documentada a posteriori para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional”*⁴⁸.

Hasta aquí hemos hablado, más bien, de lo que sería aportar la información cómo document privado. Sin embargo, también es preciso mencionar la posibilidad de hacerlo mediante documento público (art. 267 LEC). En estos casos, se suele aportar el acta notarial de la prueba digital. En ella, el Notario protocoliza en acta la impresión que la parte ha realizado en documento privado del contenido concreto que quiere incorporar como prueba. En muchos casos, se aporta un acta de presencia que implica que el Notario deberá acudir para, desde el ordenador, acceder a los correos electrónicos, sitios web, redes sociales o archivos que sean necesarios.

b) Como documento electrónico o prueba de instrumentos

La Ley 59/2003, de 19 de diciembre, de firma electrónica (en lo sucesivo, LFE) define en su artículo 3.5 el concepto de documento electrónico de la siguiente forma: *“se entiende por documento electrónico aquella información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado”*.

En estos casos lo que se incorpora al proceso es el soporte en sí, es decir, un pendrive, un DVD, un CD u otros medios que permitan el almacenamiento de datos. Las partes pueden aportar todos los medios y soportes que consideren necesarios siempre y cuando se respeten las garantías del proceso y que el juzgado o tribunal tenga los

⁴⁸ Tribunal Supremo (Sala Segunda, de lo penal), Sentencia núm. 300/2015, de 19 de mayo.

medios para reproducirlos.⁴⁹ En este sentido, el art. 384 LEC prevé que los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso serán examinados por el tribunal por los medios que la parte proponente aporte o que el Tribunal disponga emplear⁵⁰.

El proceso más en concreto es el siguiente: se hará entrega en el juzgado de la grabación de las imágenes o sonidos en el soporte en que se encuentren (un CD, DVD, pendrive o semejante) o en cualquier instrumento, por ejemplo un teléfono móvil. Suele ayudar la entrega, al mismo tiempo, de una transcripción escrita de las palabras⁵¹.

c) Mediante el reconocimiento judicial

Este medio de prueba implica el examen de la prueba directamente por el órgano judicial competente. Puede llevarse a cabo en la sede judicial o donde se encuentre el soporte electrónico, por ejemplo el ordenador, que precisa ser examinado y en el cual se almacena la información de interés⁵².

d) Mediante el interrogatorio

En este último caso simplemente decir que será durante el interrogatorio de las partes, de los testigos o de los peritos.

⁴⁹ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 54-56.

⁵⁰ Queral Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, Bosch Editor, 2011, p. 375-377.

⁵¹ Audiencia Provincial de Barcelona, secc. 13a, Sentencia núm. 113346/2007, de 2 de mayo de 2007, (La Ley). “Aportación prueba medios audiovisuales: sigue el mismo régimen que la prueba documental, con el mismo fundamento; la parte que proponga la prueba, podrá acompañar (potestativo) con el soporte transcripción escrita de las palabras contenidas en el soporte que se trate y que resulten relevantes para el caso”.

⁵² Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018, p. 451.

e) Mediante la prueba pericial

La prueba pericial es objeto de análisis al final de este cuarto punto, al tratar la cuestión de la verificación. A continuación analizaremos la prueba pericial en cuanto a medio de prueba digital; en acambio, en el análisis de la verificación abordaremos la cuestión de la prueba pericial, más bien, como la manera de probar y garantizar la no manipulación de la información que se quiere probar ante el órgano judicial.

Podemos decir, a grandes rasgos, que la prueba pericial (arts. 335 y 352 LEC) tiene como eje fundamental la presencia de un perito que se caracteriza por tener y aportar unos conocimientos especializados esenciales para que probar la autenticidad y veracidad de los hechos objeto de prueba. El perito elaborará, posteriormente, un dictamen que aportará al proceso.

La prueba pericial informática puede ser aportada al proceso de estas formas:

- Mediante un dictamen pericial elaborado por el perito cuando éste ha sido llamado por las partes
- Mediante el dictamen pericial que elabore el perito designado por el Juez
- Mediante un informe elaborado por una institución o entidad oficial especializada en la materia que se esté tratando (esto tiene más relevancia en el proceso penal).

Como ya hemos dicho, la pericial se puede aportar como prueba independiente o como prueba complementaria a otra. En este último caso la prueba pericial informática se suele presentar con frecuencia para acreditar la autenticidad de la información contenida en el soporte electrónico aportado.

3.3.2. Otros requisitos para la aportación

Para la correcta aportación de la prueba electrónica o digital existen, además, otros requisitos. Los artículos 382 y ss LEC no contienen ninguna previsión al respecto. Tampoco lo hacen los artículos 273-280 LEC. Simplemente cabe mencionar que una correcta aportación de esta prueba requiere el traslado de copias a la parte contraria.

En cuanto a los medios de prueba audiovisuales, la LEC establece la posibilidad de aportar la transcripción escrita del contenido del soporte aportado. La transcripción también la puede ordenar el propio juez o tribunal. Por el contrario, esto no se contempla para los instrumentos o soportes informáticos. En todo caso, es una facultad de la parte, que puede ser de gran utilidad sin perjuicio de que el tribunal o el juez examinen directamente el contenido del soporte que se aporta al proceso para poder hacer una valoración lo más precisa y correcta posible. La transcripción que proporcione la parte no supe la reproducción y examen y, por supuesto, su omisión no tendrá ningún tipo de consecuencia.

Puede darse el caso de que el medio de prueba que se quiere aportar no esté a disposición de quien pretende llevar a cabo su proposición sino que esté en manos de la parte contraria o de un tercero. Esta situación se prevé en la LEC y se da una solución, pero no existe previsión semejante para la prueba electrónica. La doctrina mayoritaria opta por aplicar esos preceptos (arts. 328 a 334 LEC) de manera analógica. Sin embargo, tal y como estamos viendo, la prueba electrónica o digital presenta muchas especialidades y complicaciones por lo que serían necesarios matices y apuntes al respecto. Sobre todo, el mayor problema surgiría en cuanto a la manipulación o alteración por la parte contraria o el tercero (a quienes puede no interesar que la otra parte aporte esa información). Así, habría que tomar fuertes medidas que garantizaran el buen estado, la veracidad y la autenticidad de esos medios tales como la custodia por el Secretario Judicial.

3.3.3. Conservación y verificación

a) Verificación: la prueba pericial

La prueba pericial es un medio concreto de prueba cuya regulación se encuentra, principalmente, entre los artículos 335 y 352 LEC. Es una prueba de carácter personal puesto que se basa en la presencia de una persona, el perito, quien tiene conocimientos especializados de los que el juez carece y que los aporta al proceso para una mejor valoración de los hechos por parte del órgano jurisdiccional. De este

modo, el perito debe ser⁵³ una persona ajena al proceso y que no haya sido traído al proceso por su involucración en los hechos sino por poseer esos conocimientos técnicos especializados que ayudarán al juez a valorar los hechos y a adquirir certeza sobre éstos⁵⁴.

Es esencial que el perito lleve a cabo su labor y elabore el dictamen que posteriormente presentará ante el órgano jurisdiccional competente desde la imparcialidad y la objetividad. Esto es de elevada importancia dada la labor de auxilio y apoyo para la que se le ha llamado. Por esto, la ley da a las partes la posibilidad de recusar al perito cuando crean conveniente manifestar cualquier circunstancia que ponga en duda su imparcialidad. El perito deberá abstenerse cuando concurra una causa de recusación.

El perito puede ser designado y llamado al proceso por las partes cuando éstas consideren que es necesaria la intervención de alguien con unos conocimientos determinados. Podrán hacerlo en la demanda o contestación a la demanda, antes de la audiencia previa o antes del juicio. Sin embargo, el tribunal puede, de oficio, acordar la presencia de los peritos en el juicio.

Respecto de su valoración, podemos decir que la realiza el juez libremente en concordancia con el artículo 348 LEC. Ahora bien, si la prueba pericial se hace por falta de conocimientos especializados del juez, ¿hasta que punto es preciso que sea él quien se encargue de la valoración? La mayoría de la doctrina opina que a pesar de que el juez carezca de esos conocimientos especializados y no pueda verificar las operaciones periciales, sigue pudiendo enjuiciar su corrección y resultados. Es más, la jurisprudencia entiende que esta cuestión no tiene relevancia alguna⁵⁵.

⁵⁴ Montero Aroca J, Gómez Colomer JL, Barona Vilar S, Calderón Cuadrado MP; *Derecho Jurisdiccional II Proceso Civil*, Tirant Lo Blanch; Valencia, 2014.

⁵⁵ González Pillo, E., Iglesias Canle, I., “La prueba pericial en la nueva Ley de Enjuiciamiento Civil”, *Revista Xuridica Galega*, 2000, (www.rexurga.es).

En este caso, debemos referirnos en concreto a la prueba pericial informática. Simplemente añadiremos que los conocimientos a aportar por el perito⁵⁶ serán de carácter técnico y permitirán la aportación de información y datos que se hallen en sistemas informáticos o en dispositivos electrónicos o digitales. Un ejemplo sería la labor del perito consistente en verificar y acreditar la autenticidad de conversaciones mantenidas a través de aplicaciones de mensajería instantánea tales como WhatsApp, de los correos electrónicos, o incluso, la acreditación de sabotajes y manipulación de sistemas informáticos.

Sin más dilación, diremos que la prueba pericial informática puede acceder al proceso de tres modos: en primer lugar, mediante un dictamen pericial ya elaborado en los casos en los que, bien el demandante o bien el demandado, han designado a instancia de parte a un perito; en segundo lugar, mediante el dictamen pericial que elabore el perito designado por el Juez a instancia de una o varias partes; y en tercer lugar, mediante un informe elaborado por una institución o entidad oficial especializada en la materia que se esté tratando (esto tiene más relevancia en el proceso penal).

¿Cómo se relaciona la prueba pericial informática con otros medios probatorios? La prueba pericial se puede practicar como prueba complementaria a otro medio probatorio, por ejemplo cuando se aporta un documento electrónico con información y se hace la prueba pericial para acreditar su veracidad y autenticidad. Sin embargo, también se puede practicar como prueba autónoma, independiente. En este caso caben dos escenarios: los datos de interés pueden encontrarse en un dispositivo electrónico o en una transmisión de redes de telecomunicaciones entre otras y ser de difícil acceso para alguien sin conocimientos técnicos. Por ejemplo, cuando se quiere saber si alguien ha obtenido datos sin permiso de un dispositivo electrónico ajeno, cuando se quieren averiguar el número de visitas a una determinada página web o cuando los datos se encuentran en archivos ocultos, encriptados o eliminados. El otro escenario nos remite a situaciones en las que los datos no son de difícil acceso y, por tanto, no sería necesaria la intervención de un perito, sería suficiente con aportar datos que

⁵⁶ Audiencia Provincial de Barcelona, secc. 7a, Sentencia núm. 317/2008, de 29 de enero. “Designación judicial de perito informático de entre una de las tres posibilidades ofrecidas por la denunciante: lista de peritos judiciales; Asociación de Doctores, Licenciados e Ingenieros en Informática (ALI): o Asociación de Técnicos en Informática (ATI)”.

facilitaran la navegación por Internet del juez o con aportar los medios electrónicos adecuados (DVDs, fotos...).

Como hemos indicado, la prueba pericial informática⁵⁷ será precisa cuando:

- se necesiten conocimientos especializados de carácter técnico para acceder a la información de un dispositivo porque el acceso sea difícil, oculto o encriptado; o
- se deba acreditar la autenticidad, veracidad e integridad del contenido de la información.⁵⁸

En este sentido, parece conveniente dar el siguiente ejemplo: SAP Cádiz, secc. 2ª, de 25 de febrero de 2008 sobre la *“Impugnación de la autenticidad del documento con firma electrónica avanzada: la autenticación consiste en la práctica de cualquier medio de prueba que resulte útil y pertinente, pudiendo practicarse prueba pericial que acredite que el medio de prueba no ha sido manipulado, o prueba testifical con el autor del documento aportado”*.

Es llegados a este punto cuando debemos hablar de **la cadena de custodia**.

b) Conservación: la cadena de custodia

Por cadena de custodia entendemos el procedimiento que permite verificar la identidad, integridad y autenticidad de los hechos relevantes para el asunto que se trata en el proceso en cuestión desde que son encontrados hasta que son, efectivamente, aportados al proceso en forma de prueba⁵⁹. Este proceso debe estar siempre debidamente documentado.

En cuando a la prueba pericial informática, la garantía de la cadena de custodia presenta algunas complicaciones ya que es difícil demostrar que la información que se

⁵⁷ Rayón Ballesteros, MC., Gómez Hernández, JA., *“Ciberdelitos: Particularidades en su investigación y enjuiciamiento”*, Anuario Jurídico y Económico Escorialense, XLVII (2014).

⁵⁸ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 68.

⁵⁹ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 70.

presenta ante el Tribunal o el Juez es la misma que la que fuera incautada o aprehendida en un primer momento.

Como recuerda la STC 170/2003, de 29 de septiembre y a la luz de la interpretación del artículo 338 LEC, se deben cumplir una serie de condiciones en cuanto a la cadena de custodia. Así, debe existir una descripción detallada del material y, si fuera necesario, el material en cuestión debe ser precintado. Se debe siempre velar por el mantenimiento y evitar el deterioro por lo que el lugar de custodia debe ser elegido adecuadamente. Además, es importante el control judicial durante la recogida y la custodia. Si esto no se cumpliera, se podría alegar falta de validez. Por tanto, recordamos que el principal problema de la cadena de custodia nace en la dificultad de garantizar que aquello que se traslada como prueba, se incorpora al proceso y, posteriormente, se analiza o visiona en la práctica de la prueba durante el juicio, es lo mismo en todo momento.

Ahora bien, la vulneración de la cadena de custodia no constituye por sí misma una vulneración de derechos fundamentales como el derecho de defensa, que solo se daría cuando se admitieran y valoraran pruebas recogidas violando los derechos de alguna de las partes y sin respetar las garantías esenciales del procedimiento. Esto se debe a que lo que realmente constituye la cadena de custodia es un procedimiento de ocupación, conservación, transporte y entrega de los objetos; y por tanto, tiene un carácter, más bien, instrumental. Podríamos decir, incluso, que a pesar de un posible error en este proceso, ello no supondría un sustento racional y suficiente para sospechar que las entregas no fueran las originales. Podemos mencionar a estos efectos la STS 629/2011, de 23 de junio y STS 776/2001, de 20 de julio.

Para terminar, conviene destacar una de las fases más características de la prueba pericial informática: el clonado de datos y cálculo de hash. Tras obtener los datos y la información y antes de la elaboración y presentación del dictamen pericial, se realizan las dos actuaciones ya mencionadas. En primer lugar, el clonado de datos consiste en hacer una copia bit a bit, es decir, coloquialmente, una copia exacta o copia 'espejo', de la información original. De este modo, tendremos la información y datos originales, que se preservarán hasta el juicio, y una copia, el clonado, que empleará el perito para su dictamen. En segundo lugar, el código hash es una función basada en

un algoritmo y operaciones matemáticas e informáticas que permite verificar que, efectivamente, los datos que se encontraban en el dispositivo no han sido manipulados⁶⁰. El resultado de esa operación matemática nos da un resultado de 32 dígitos aproximadamente y en el caso de que se modificara un solo bit de los datos o información objeto de prueba, ese resultado variaría en alguno de sus dígitos, demostrando que ha sido objeto de manipulación. A este respecto existen determinadas normas internacionales: RFC 3227 (2002) Directrices para la recopilación de evidencias y su almacenamiento; ISO/IEC 27037 (2012) Guía para la Identificación, recolección, adquisición, y preservación de evidencia digital⁶¹. Como conclusión a este apartado podemos dar mención a dos resoluciones: SAP Cádiz, Secc. 2ª, de 25 de enero de 2008 sobre la prueba documental que consiste “*en copia privada obtenida de documento electrónico (e-mails): se distingue entre el original – que se encuentra en el registro informático– y la copia –obtenida a través de la impresora e incorporada a las actuaciones en soporte papel*”; y SAP Barcelona, Secc. 7ª, de 29 de enero de 2008 sobre las medidas “*para garantizar la custodia de un material informático incautado por la policía*”.

3.4. Admisión de la prueba digital

Pertinencia, utilidad y legalidad son los tres caracteres o requisitos que impone la LEC para la admisión de la prueba propuesta e incorporada al proceso en condiciones normales. Pese a todas las particularidades que caracterizan a la prueba digital, no se han establecido unos requisitos determinados para este tipo de prueba en concreto.

Ante este vacío legal y siguiendo a Francis LEFEBVRE podemos decir que “un tribunal admitirá una prueba digital cuando:

- se identifique el equipo del que procede el documento electrónico y se demuestre su correcto funcionamiento

⁶⁰ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 71,72.

⁶¹ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 83.

- se demuestre que los datos introducidos lo hayan sido conforme a un programa que refleje la exactitud de dicho proceso, y
- se pruebe de forma razonable que el procesamiento, almacenaje y salida de datos se ha realizado de forma fiable

El juicio de admisibilidad basado en estas cuestiones puede presentar complejidad técnica, por lo que al juez le puede resultar útil contar con un dictamen pericial⁶² (que será objeto de análisis en apartados posteriores de este trabajo).

3.5. Práctica de la prueba digital

La prueba digital se practicará en la sede del tribunal, a excepción de los casos en los que, por la naturaleza de ésta, deba practicarse en otro lugar (art. 129.1 LEC). La práctica de la prueba digital no presenta ninguna especialidad más que cuando se precisa de un instrumento técnico para acceder a la información que se contiene en un soporte electrónico, es decir, cuando estamos ante una prueba de instrumentos.

Puede ser que la prueba esté en medios audiovisuales, en cuyo caso simplemente habría que reproducirlos. Para ello es inexcusable la presencia del juez. Otra opción es que se hayan aportado instrumentos informáticos en los cuales se ha archivado la información en cuestión. En estos casos, el tribunal deberá examinar dichos soportes e instrumentos con los medios de los que disponga o, cuando proceda, con los que las partes hayan proporcionado.

La práctica de la prueba puede tener lugar en diferentes momentos del proceso judicial. En primer lugar, las diligencias preliminares. Las partes pueden solicitar que el tribunal lleve a cabo una serie de actuaciones previas al proceso. En segundo lugar, la prueba anticipada que permite la práctica de aquellas pruebas por las cuales exista un miedo fundado de que, con el paso del tiempo, puedan desaparecer o perder su objeto. En tercer lugar, la práctica ordinaria la cual tendría lugar en el propio acto del juicio. Por último y en cuarto lugar, las diligencias finales que deben ser acordadas y practicadas en el plazo para dictar sentencia con suspensión de ésta. Su objeto son las

⁶² Lefebvre, F., *Derecho de las Nuevas Tecnologías*, Memento Práctico, Écija, 2017-2018, p. 452.

pruebas admitidas pero que no han podido ser practicadas por causas que no se deben a la parte que las propone, o a pruebas que se desconocían previamente.

3.6. Valoración de la prueba digital

La valoración de la prueba consiste en otorgarle credibilidad a la información y datos presentados por las partes. La regla que rige en nuestro sistema es la de la libre valoración por el juez o tribunal. A la luz del artículo 348.3 LEC podemos decir que se deja la valoración de las pruebas a “*las reglas de la sana crítica*”⁶³ del juez o tribunal en cuestión.

La libre valoración implica que no siempre, por Ley, el juez debe tener por probados los hechos que surjan de la prueba digital, a excepción de los plasmados en documento público electrónico. Además, no hay unos requisitos a cumplir para que la prueba digital cuente con eficacia probatoria, al contrario, toda prueba digital podrá desplegar efectos pero estaremos sujetos al interrogante de la verosimilitud o eficacia que el juez le de en el caso concreto. Cuando la LEC se refiere a las reglas de la sana crítica no se refiere a otra cosa que no sea el criterio racional del juez, es decir, una valoración basada en la lógica, la experiencia y, por supuesto, en los conocimientos científicos específicos.

La libre valoración deberá tener como fondo siempre la autenticidad del origen de la información y la integridad del contenido, como hemos venido indicando en las dos fases anteriores: obtención de la información e incorporación de ésta al proceso. Así, lo recuerdan tanto la LEC en su artículo 382.2 al referirse a “*la autenticidad y exactitud de lo reproducido*”, y la LOPJ en su artículo 230.2 al mencionar que “*los documentos emitidos por los medios anteriores, cualquiera sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad [...]*”.

⁶³ Lefebvre, F., *Derecho de las Nuevas Tecnologías*, Memento Práctico, Écija, 2017-2018, p. 453.

En la libre valoración, ¿qué se tiene en por autenticidad en el origen e integridad en el contenido? En cuanto a la autenticidad, se tendrá en cuenta el origen de los datos, es decir, se dará importancia a la fuente de la que proviene esa información. En cuanto a la integridad el juez tendrá en cuenta que los datos no se hayan alterado o manipulado sin autorización.

Para facilitar esta labor de valoración la LEC en sus artículos 382 y 384 prevé que la parte proponente pueda aportar dictámenes y medios de prueba instrumentales junto con el medio electrónico. Del mismo modo podrá hacerlo la parte contraria cuando cuestione la autenticidad y exactitud de lo reproducido⁶⁴.

El final de esta fase de valoración llega con la motivación de la valoración de la prueba que debe realizar el juez. En este punto, solo cabe precisar que desde el punto de vista de nuestro Tribunal Constitucional, el hecho de la obligación de los jueces y tribunales de motivar las decisiones y resoluciones, forma parte del derecho a la tutela judicial efectiva. Además, la motivación de las resoluciones judiciales aparece en el artículo 120.3 CE.

4. LICITUD E ILICITUD DE LA PRUEBA DIGITAL. ALUSIÓN A DETERMINADOS DERECHOS FUNDAMENTALES

En este apartado trataremos una de las cuestiones que, en cuanto a la prueba digital, han dado lugar a más controversia y jurisprudencia: la vulneración de determinados derechos fundamentales en la obtención de la prueba digital.

Los derechos fundamentales no limitan su actuación y vigencia a las relaciones entre los individuos y los poderes públicos del Estado; por el contrario, también actúan en las relaciones entre particulares. Así lo recuerda el Tribunal Constitucional en su sentencia STC 18/1984, de 7 de febrero, en la que dictamina, aludiendo al art. 9.3

⁶⁴ Queral Carbonell, A., “La prueba electrónica”, Capítulo III Proposición, admisión y práctica de la prueba electrónica, Serie de Estudios Prácticos sobre los Medios de Prueba, ESADE, 2011, BOSCH EDITOR, p. 378.

CE⁶⁵, lo que sigue: “*esta concretización de la ley suprema no debe interpretarse en el sentido de que sólo se sea titular de los derechos fundamentales y libertades públicas en relación con los poderes públicos, dado que en un Estado social de derecho como el que consagra el art. 1 CE no puede sostenerse con carácter general que el titular de tales derechos no lo sea en la vida social [...]*”. Este fragmento se refiere a la afirmación del 9.3 CE en cuanto a que la Constitución velará por el bien de los particulares ante la arbitrariedad de los poderes públicos.

El artículo 11.1 Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985) (en lo sucesivo, LOPJ), dice así: “*En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando derechos o libertades fundamentales*”. Entendemos así que la ley no pretende declarar ilícitas determinadas pruebas sino todas aquellas que, al obtenerse, hayan violentado los derechos subjetivos de las personas, así como los derechos que nuestra Constitución considera como fundamentales.

A continuación, analizaremos algunos de los derechos fundamentales que, en sede de obtención de la prueba digital, se muestran más vulnerables. Estos son:

- El derecho a la intimidad
- El secreto de las comunicaciones
- La protección de datos personales

4.1. El derecho a la intimidad personal y familiar

El derecho a la intimidad se enmarca dentro de los derechos fundamentales recogidos por nuestra Constitución y es en el artículo 18.1 de dicha norma donde encontramos su regulación. En palabras del Tribunal Constitucional⁶⁶ “*el derecho fundamental a la intimidad reconocido por el artículo 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto a su dignidad como*

⁶⁵ Art 9.3 CE: “*La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos*”.

⁶⁶ Tribunal Constitucional (Sala segunda), sentencia núm. 115/2000, de 10 de mayo de 2000.

persona, frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares”. Asimismo, el Convenio Europeo de Derechos Humanos prevé en su artículo 8.1 la existencia del derecho al respeto de la esfera privada.

Lo que ambos preceptos pretenden garantizar es el secreto y el respeto hacia la esfera de vida personal de cada uno (STC 115/2013, de 9 mayo; STC 159/2009, de 29 de junio). En palabras de Francis LEFEBVRE “*en el concepto de intimidad palpita la idea de evitar la injerencia de terceros en la vida privada que subyace desde la formulación del derecho: ‘el derecho a la intimidad es el derecho a ser dejado en paz*”⁶⁷.

En sede de la prueba tecnológica, y en el marco de la sociedad de la información, cabe decir que las tecnologías de la información y la comunicación han incrementado el riesgo de que nuestra intimidad se vea violentada con mucha más facilidad que antes.

Podemos dividir la intromisión ilegítima en dos grandes grupos: por un lado, la intrusión en la vida privada de la persona en el que encontraríamos la intromisión en su hogar, la instalación de micrófonos u otros dispositivos para grabar el contenido de ciertas conversaciones privadas o la intervención de conversaciones telefónicas. Por otro lado, encontraríamos la divulgación pública de hechos privados⁶⁸.

Toda la información contenida en nuestros dispositivos electrónicos afecta a nuestra intimidad personal. Por esto, todas las garantías que permiten la injerencia en este derecho fundamental para así poder obtener datos que puedan ser incorporados al proceso como prueba, son de aplicación en todas las jurisdicciones. Si se incumplen estas garantías y requisitos la prueba será ilícita y, por tanto, nula⁶⁹. A estos efectos,

⁶⁷ Lefebvre, F., *Derecho de las Nuevas Tecnologías*, Memento Práctico, Écija, 2017-2018, p. 337.

⁶⁸ Art. 7 LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

⁶⁹ Asencio Mellado, JM., “Prueba ilícita: declaración y efectos”, *Revista General de Derecho*, 26 (2012), p. 15.

podemos citar una sentencia del Tribunal Constitucional del año 2011 que dice así: *“el cúmulo de la información que se almacena en un ordenador personal, entre otros datos sobre su vida privada y profesional, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. [...] Cuando el titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico [...] está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre salud, orientaciones sexuales, etc.”.*

Además, en referencia exclusiva a las actividades llevadas a cabo en Internet, se puede afirmar que todo lo que difundimos en Internet es de carácter público y que, de hecho, al publicarlo estamos dando de alguna forma nuestro consentimiento tácito a que esas informaciones sean públicas.

Las comunicaciones en Internet se pueden realizar de dos modos: en canal abierto o en canal cerrado. Las comunicaciones en canal abierto implican que la información se inserta en las webs y es accesible al público de manera que el conocimiento de esos datos no afecta a los derechos fundamentales de quien los cuelga. Por el contrario, en las comunicaciones en canal cerrado estamos ante un intercambio de información vía Internet pero entre personas determinadas. En este caso sí que tendrá relevancia el hecho de que un tercero ajeno a esa comunicación tenga acceso y conocimiento de la información que en ella se transmite. Dice Eloy Velasco Núñez que “el acceso a Internet no afecta a derechos fundamentales, pues ni es privado ni íntimo lo que se deja allí, ni se trata de una telecomunicación formalmente protegida cuyo secreto deba guardarse⁷⁰ [...]”.

¿Cómo se puede investigar el contenido colgado o consultado en Internet? Mediante los rastreos informáticos llevados a cabo por la policía. Estos rastreos no vulneran los derechos fundamentales.

⁷⁰ Velasco Núñez, E., “Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías”, El Derecho, Revista de Jurisprudencia, núm. 4, 24 de febrero de 2011.

Por último, también hay que hacer una mención a los datos de navegación web. Estos datos son los que permiten acceder al contenido de navegación que ha realizado una persona. Es decir, permiten conocer qué contenidos, de los disponibles en la web, han sido consultados por una determinada persona. Al no ser una comunicación entre personas determinadas no afecta al derecho de secreto en las comunicaciones pero no se puede negar que estos datos pueden contener información relevante sobre la vida íntima y privada de alguien. Por esto, incluimos este apartado en el estudio del derecho a la intimidad en la prueba digital. Es útil a este respecto la mención del Caso Copland⁷¹. Ésta hace una referencia clara y expresa a la protección de los correos electrónicos que un trabajador envía y recibe en el marco de su puesto de trabajo, así como a la protección de la “información derivada del seguimiento del uso personal de Internet”. Así, es fácil concluir que el acceso a los datos de navegación que pueden hallarse en los dispositivos electrónicos de una persona sí afecta al derecho a la intimidad de ésta. Por último, no podemos terminar este apartado sin hacer una breve referencia a la ‘política de Cookies’ tan presente hoy en día en cualquier sitio web al que accedemos. Las ‘cookies’ o galletas informáticas son, de acuerdo con la definición proporcionada por el magistrado Joaquín Delgado Martín en su libro *“Investigación tecnológica y prueba digital en todas las jurisdicciones”*⁷², breves informaciones que emite un sitio web que queda almacenada en el navegador del usuario, y que implica que el sitio web pueda determinar o consultar la actividad previa del citado usuario.

Dice Francis LEFEBVRE que aquella persona que infringe o vulnera los derechos de la personalidad de otra “sólo debería ser sancionado por su acción y no por la divulgación posterior que se haga de dicho acto a través de internet o las redes sociales, cuyos responsables serán los autores de dicha divulgación”.

Para dar por terminado este subapartado, mencionaremos dos casos: el primero, plasmado en la STSJ Madrid, Sala de lo social, secc. 2ª, sentencia núm. 43/2998, de

⁷¹ Sentencia Tribunal Europeo de Derechos Humanos, Secc. 4ª, Demanda 62617/00, de 3 de julio de 2007, Caso Copland contra Reino Unido, Portal europeo e-justice, consultado el 15 de marzo de 2017.

⁷² Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 110.

16 de enero⁷³, y el segundo plasmado en la STC, Sala Segunda, sentencia núm. 212/2013, de 16 de diciembre⁷⁴.

4.2. El derecho de secreto de las comunicaciones

El art. 18.3 CE prevé la existencia del derecho al secreto de comunicaciones cuya principal razón de ser la encontramos en el respeto hacia las comunicaciones de otros que nos son ajenas. El Tribunal Constitucional afirmó en el año 2013 que *“el objeto directo de protección del art. 18.3 CE es el proceso de comunicación en libertad y no por sí solo el mensaje transmitido, cuyo contenido puede ser banal o de notorio interés público”* (STC 170/2013, de 7 de noviembre⁷⁵).

Por tanto, cabe distinguir tres elementos que componen este derecho de las comunicaciones: primero, la transmisión de información o contenido; a continuación, que ésta sea entre dos o más personas determinadas o determinables; y, por último, la intermediación de un tercero con obligación de confidencialidad. Este último elemento es el que más dudas puede llegar a levantar. Simplemente nos referimos a que la comunicación se realiza mediante un prestador de servicio de comunicación que está vinculado a las personas que forman esa comunicación, siempre desde un vínculo de confidencialidad⁷⁶.

Hay supuestos que quedan fuera del ámbito de aplicación del derecho de secreto en las comunicaciones. El ejemplo más claro serían las comunicaciones abiertas en las que no hay confidencialidad del canal (televisión, comunicaciones radiofónicas).

⁷³ STSJ Madrid, Sala de lo social, secc. 2ª, sentencia núm. 43/2998, de 16 de enero, que establece que *“sí se considera vulneración del derecho a la intimidad del trabajador la realización de un registro en el ordenador sin una previa advertencia que tal control podía efectuarse”*.

⁷⁴ STC, Sala Segunda, sentencia núm. 212/2013, de 16 de diciembre: *“Pertinencia de la prueba y arbitrio judicial: proceso por despido: denegación del visionado de las imágenes contenidas en el DVD que había sido admitido como prueba, así como de las preguntas del Letrado de la demandante a su cliente: imposibilidad de probar el sustrato fáctico de la lesión del derecho a la intimidad y de someter a escrutinio la credibilidad de los testigos: indefensión existente”*.

⁷⁵ Tribunal Constitucional, Sala Primera, Sentencia núm. 170/2013, de 7 de noviembre. BOE núm. 267, de 7 de noviembre de 2013.

⁷⁶ Rodríguez Lainz, J.L., “Internet de los objetos y secreto de las comunicaciones”, Diario La Ley, nº 8034, Doctrina, 2013.

A continuación procederemos a examinar la relación con la prueba digital en concreto. Existen dos casos en los que el derecho del secreto de las comunicaciones se vería afectado: primeramente, el acceso a datos transmitidos por redes en procesos de comunicación; en segundo lugar, el acceso a información que se ha colgado en Internet pero en canal cerrado, es decir, destinado a unas personas determinadas.

Más dudas suscita el caso de acceder a datos que encontremos en un dispositivo electrónico. Aquí vemos una clara intromisión en el derecho a la intimidad pero es más controvertida y dependería del caso concreto la vulneración del derecho de secreto de las comunicaciones. Ahora bien, en el caso de obtener información a través de paginas web estaríamos totalmente fuera del ámbito de aplicación de este derecho por ser un canal de comunicación abierto⁷⁷.

Algunos ejemplos jurisprudenciales son: SAP, Barcelona, secc. 15a, sentencia núm. 339/2008 de 23 de septiembre⁷⁸ y SAP Badajoz, secc. 1a, sentencia núm. 26/2011 de 28 de junio⁷⁹.

4.3. La protección de datos personales

El derecho a la protección de datos personales, plasmado en el artículo 18.4 CE y en la Directiva 95/46/CE, es el poder que tiene una persona sobre el control, el uso y el destino de sus datos personales, otorgado por el ordenamiento jurídico. La STC 292/2000, de 30 de noviembre, lo define de manera muy acertada como sigue: *“el derecho a la protección de datos atribuye al titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que*

⁷⁷ Sentencia del Tribunal Europeo de Derechos Humanos, Petición núm. 48539/99, de 5 de noviembre de 2002, Caso Allen contra Reino Unido. Portal europeo e-justice. Conversaciones observadas o grabadas por agentes estatales, aún cuando alguno de los interlocutores hubiera admitido la injerencia del Estado.

⁷⁸ SAP, Barcelona, secc. 15a, sentencia núm. 339/2008 de 23 de septiembre. *“Inexistente violación del derecho al secreto de las comunicaciones, ausencia de interferencia en ningún proceso de comunicación ajeno”*.

⁷⁹ SAP Badajoz, secc. 1a, sentencia núm. 26/2011 de 28 de junio: *“Conductas realizadas por autoridad o funcionario público prevaleciendo de su cargo. Ausencia de pruebas al haber sido declaradas nulas la obtenidas con violación del derecho fundamental al secreto de las comunicaciones”*.

no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho: garantizar a la persona un poder de control sobre sus datos personales [...]. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.[...]". Además, en este ámbito contamos en nuestro entorno legal con la Ley Órgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

Son muchos los datos personales que resultan de importancia de cara al proceso, más concretamente para la prueba. Se podrán aportar al proceso los datos de carácter personal que se encuentren dentro del ámbito establecido por la ya mencionada LOPD⁸⁰.

La problemática de cara a la prueba digital es que ésta se consiga violando el derecho de protección de datos personales. La obtención de datos puede darse de dos maneras⁸¹:

- Mediante el consentimiento del titular: simplemente añadir que por consentimiento se entenderá cualquier manifestación de voluntad expresada de manera libre, inequívoca, específica e informada. En ella el interesado debe permitir el uso de los datos personales que a él le incumban (art. 3 LOPD). Sin embargo, el art. 6 de la misma ley establece una serie de casos en los que se permite la obtención de un dato personal sin consentimiento⁸².

⁸⁰ García Moreno, S., "Nuevo marco jurídico europeo: novedades conocidas y no tan conocidas", Diario La Ley, nº 8691, 28 de enero de 2016.

⁸¹ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 135.

⁸² Art. 6.2 LOPD: "No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

- Mediante la cesión del dato obtenido legítimamente por un tercero: en estos casos, el conflicto más habitual se da cuando un particular o una entidad ha obtenido legítimamente un dato personal de otra persona y se quiere ceder éste a un tercero para que lo aporte como prueba. Para que esto se permita se deben cumplir los requisitos de los art. 11 y 21 LOPD. Lo principal es el previo consentimiento del interesado que se excluye en determinados supuestos enumerados en el apartado 2 del art. 11⁸³.

Como ejemplos jurisprudenciales acudiremos a estas dos resoluciones: STC, sala primera, sentencia núm. 96/2012, de 7 de mayo⁸⁴ y STS Sala 3ª, sentencia núm. 3896/2012, de 3 de octubre⁸⁵.

Con carácter general, cuando los datos se han obtenido de forma lícita no hay más problemas en relación con la prueba digital. Si que es cierto que existen hoy en día muchas técnicas de análisis automatizado de datos cuya conservación puede además extenderse en el tiempo. Gracias a estos avances metodológicos se prevén grandes avances de cara a la investigación y verificación de pruebas digitales logrando la salvaguardia de los derechos de la personalidad y fundamentales⁸⁶.

⁸³ Art. 11.2 LOPD: “a) Cuando la cesión está autorizada en una Ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica”.

⁸⁴ STC, sala primera, sentencia núm. 96/2012, de 7 de mayo: “Existe una vulneración material del art. 18.4 CE, que implica la lesión del derecho a la tutela judicial efectiva (art. 24.1 CE) de la entidad bancaria demandante de amparo; y declara la nulidad del auto del Juzgado de Primera Instancia núm. 87 de Madrid y otras actuaciones procesales [...]”.

⁸⁵ STS Sala 3ª, sentencia núm. 3896/2012, de 3 de octubre: “STS estima que las direcciones de IP son datos personales, en el sentido del art. 3 LOPD. [...] No resulta de aplicación la exención del art. 5 LOPD y tampoco concurre el consentimiento tácito del interesado para la recogida de datos [...]”.

⁸⁶ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p. 144.

4.4. La prueba digital ilícita en el proceso civil

Como se explica en el apartado anterior, cualquier aportación al proceso de las fuentes de la prueba digital debe hacerse con pleno respeto a los derechos fundamentales. Así, una prueba ilícita, obtenida contraviniendo las garantías y derechos de la parte contraria será considerada nula. Esa nulidad se extenderá a las pruebas con las que tenga una conexión de antijuridicidad. La ilicitud la puede apreciar el juez o las partes⁸⁷.

Declaración de nulidad de oficio por el juez (vía art. 287.1,2 LEC): la planteará el propio juez que dará audiencia a las partes. Cuando proceda, se practicarán las pruebas pertinentes para poder aclarar dicha ilicitud. El juez dará a conocer su decisión antes de la práctica de la prueba, en el acto de juicio si fuera juicio ordinario, o al inicio de la vista si fuera juicio verbal.

A instancia de parte: puede llevarse a cabo de dos modos. Por un lado, con un recurso de reposición contra la resolución a través de la que se admitió la prueba. Dicho recurso se resolverá en el acto. En caso de que el juez o tribunal desestimara el recurso, la parte que lo interpuso tendrá disponible el recurso de protesta contra esa resolución. Por otro lado, por la vía del art. 287 LEC, que establece que la parte deberán poner en conocimiento del tribunal y de las otras partes sus argumentos para considerar la ilicitud de la prueba⁸⁸.

⁸⁷ Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016, p-213-215.

⁸⁸ Pérez Cebadera, MA., La prueba ilícita en el proceso civil, Revista de Jurisprudencia El Derecho, núm. 1, 2 de junio de 2011. Disponible en http://www.elderecho.com/civil/prueba-ilicita-proceso-civil_11_283555003.html

CONCLUSIONES

Tras realizar el análisis propuesto sobre la prueba digital y su régimen general, con especial énfasis en la incorporación al proceso civil y la verificación de la misma, es preciso hacer una serie de apuntes.

En primer lugar, cabe destacar la falta de regulación expresa sobre esta materia en la LEC. Comprendiendo que resulta algo muy concreto a la par que novedoso, no podemos dejar de lado el hecho de que hoy en día, las nuevas tecnologías forman parte de la realidad cotidiana y diaria de los ciudadanos y que, por tanto, la justicia no puede quedarse atrás. Actuaciones tan simples como un mensaje de texto, una nota de voz, la firma electrónica, un correo electrónico o el registro de búsquedas de un ordenador son, muchas veces, la única manera de acreditar y probar hechos que pueden ser relevantes en un proceso judicial. Así, no sólo en beneficio de los ciudadanos, sino en beneficio de la propia administración de justicia, sería de gran utilidad un desarrollo más preciso y exhaustivo que proporcionara una mejor regulación y mayores garantías para el proceso judicial.

En segundo lugar, la falta de unicidad y claridad en cuanto a lo que se entiende por documento y soporte electrónico dan lugar a confusión y, por tanto, consideramos preciso reformular el concepto de documento en sede de legislación procesal, incorporando los avances tecnológicos y superando la concepción de que documento es aquel que se presenta únicamente en soporte papel. Más aun teniendo en cuenta que el Código Penal define el documento como *“todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica”* (art. 26). Si bien es verdad que el art. 3.5 de la Ley de Firma Electrónica sí hace referencia en concreto al documento electrónico, refiriéndose a éste como la información de naturaleza electrónica archivada en soporte electrónico y susceptible de identificación y tratamiento especial.

El hilo conductor del presente trabajo ha sido, sin duda, la LEC. Sus artículos 382 a 384 regulan los llamados medios de reproducción de palabra, sonido e imagen así como los documentos que permiten archivar y conocer datos relevantes para un proceso civil. Sin embargo, como tercer apunte, no se hace referencia a uno de los

principales problemas que nace, en especial, con la prueba digital: la obtención de la misma y su proposición, de manera expresa. Consideramos que la prueba digital, por sus características y complejidad, merece un tratamiento expreso respecto a su obtención puesto que es en ese punto donde surge una de las más importantes controversias, la vulneración de determinados derechos fundamentales. La obtención y el acceso a la información mediante dispositivos electrónicos, redes sociales, o los ya conocidos pantallazos son polémicos en cuanto al respeto a la privacidad y la protección de datos de las partes.

En otro orden de cosas, no podemos olvidar otro de los pilares de nuestro análisis, la verificación de la prueba digital. Sin duda, cualquier documento es susceptible de manipulación, pero el riesgo aumenta considerablemente en la prueba electrónica si tenemos en cuenta la dificultad de probar una manipulación en un mensaje de WhatsApp o demostrar que se han borrado datos de un ordenador, como ejemplos cotidianos y sencillos. Por esto, dos de los apartados más desarrollados dentro de la incorporación al proceso civil de la prueba digital han sido la verificación y conservación de la misma mediante la prueba pericial y la cadena de custodia. Ambas herramientas son cruciales a la hora de demostrar la autenticidad de un documento o la veracidad de los datos obtenidos y una vez más, el ordenamiento jurídico no da respuestas concretas a este respecto.

En aras de proporcionar un análisis exhaustivo y completo de la materia, hemos ido analizando todos los aspectos del régimen general de la prueba digital en cuanto al proceso civil. Se han ido tratando sucesivamente todas las cuestiones que hemos considerado relevantes tales como la obtención de la prueba electrónica sin vulnerar los derechos fundamentales de la contraparte o de terceros, su proposición e incorporación al proceso, y la forma de acreditar su veracidad y autenticidad mediante la prueba pericial y la cadena de custodia. Todo esto lo hemos sustentado proporcionando un amplio número de ejemplos jurisprudenciales, que, sin duda, aportan una visión más práctica y permiten ver el avance en la materia durante los últimos años, siendo una de nuestras principales fuentes de apoyo.

BIBLIOGRAFÍA

LEGISLACIÓN

Constitución Española, 1978.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal.

Reglamento UNCITRAL.

http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1985Recommendation.html

http://www.uncitral.org/pdf/spanish/publications/sales_publications/UNCITRAL-s.pdf

JURISPRUDENCIA

SAP de Badajoz (secc. 1ª) sentencia núm. 26/2011 de 28 de junio.[EDJ 2011/153369].

SAP de Barcelona, secc. 15a, Sentencia núm. 259/2008, de 2 de julio. [EDJ 2008/169196].

SAP de Madrid (Secc. 7ª), sentencia núm. 768/2014 de 18 de diciembre. [JUR\2015\61981].

SAP de Santa Cruz de Tenerife, secc. 4a, de 18 de noviembre de 2009. [JUR 2010/77692].

STC (Sala Primera), sentencia núm. 170/2013, de 7 de noviembre. [EDJ 2013/182887].

STC (Sala primera) sentencia núm. 96/2012, de 7 de mayo. [EDJ 2012/98391].

STC (Sala segunda), sentencia núm. 115/2000, de 10 de mayo. [RJ 2000\663].

STC (Sala Segunda), sentencia núm. 212/2013, de 16 de diciembre. [EDJ 2013/249695].

STEDH petición núm. 48539/99, de 5 de noviembre de 2002, Caso Allen contra Reino Unido. Disponible en portal europeo e-justice (www.e-justice.com).

STSJ Madrid (Sala de lo social, secc. 2ª), sentencia núm. 43/1998, de 16 de enero. [EDJ 1998/6082].

STS (Sala Segunda), sentencia núm. 300/2015, de 19 de mayo. [EDJ 2015/77775].

STS (Sala Segunda), sentencia núm. 754/2015 de 27 de noviembre. [EDJ 2015/242644].

STS (Sala de lo Penal), sentencia núm. 300/2015, de 19 de mayo. [EDJ 2015/77775].

OBRAS DOCTRINALES

Abel Lluch, X., *Prueba electrónica*, Ginés Castellet. N., *Serie de estudios prácticos sobre los medios de prueba*, ESADE, Bosch Editor, 2011.

Alonso-Cuevillas, J., *Internet y prueba civil*, Revista Jurídica de Catalunya, Vol.100, núm 4, 2001, paginas del artículo: 1071-1090.

Asencio Mellado, JM., “Prueba ilícita: declaración y efectos”, Revista General de Derecho, 26 (2012).

Bueno Aguado, CM., *Los SMS a efecto de notificación*, Revista General de Derecho Procesal, núm. 37, 2015, Iustel.

Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, Wolters Kluwer, Madrid, 2016.

García Moreno, S., “Nuevo marco jurídico europeo: novedades conocidas y no tan conocidas”, Diario La Ley, nº 8691, 28 de enero de 2016.

García Torres, ML., *La tramitación electrónica de los procedimientos judiciales, según la ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil*, Revista Internacional de Estudios de Derecho Procesal y Arbitraje, www.riedpa.com, nº3-2011,

<http://www.riedpa.com/COMU/documentos/RIEDPA31102.pdf>

González Pillo, E., Iglesias Canle, I., “La prueba pericial en la nueva Ley de Enjuiciamiento Civil”, Revista Xuridica Galega, 2000.

Herrera Joancomartí, J., *Nociones técnicas de Internet*, Peguera Poch, M., *Derecho y*

nuevas tecnologías, UOC, Barcelona.

Lefebvre, F., *Derecho de las Nuevas Tencologías*, Memento Práctico, Écija, 2017-2018.

Montero Aroca J, Gómez Colomer JL, Barona Vilar S, Calderón Cuadrado MP; *Derecho Jurisdiccional II Proceso Civil*, Tirant Lo Blanch; Valencia, 2014.

Morales García, Ó., *Derecho penal y sociedad de la información*, Peguera Poch, M., *Derecho y nuevas tecnologías*, UOC, Barcelona.

Ormazábal Sánchez, G., *El valor probatorio de la firma electrónica*, Peguera Poch, M., *Derecho y nuevas tecnologías*, UOC, Barcelona.

Peguera Poch, M., *Servicios de la sociedad de la información*, Peguera Poch, M., *Derecho y nuevas tecnologías*, UOC, Barcelona.

Pérez Cebadera, MA., La prueba ilícita en el proceso civil, Revista de Jurisprudencia El Derecho, núm. 1, 2 de junio de 2011. Disponible en <http://www.elderecho.com/civil/prueba-ilicita-proceso -civil 11 283555003.html>

Pérez Palaci E., *La prueba electrónica: Consideraciones*, Universitat Oberta de Catalunya,3 de julio de 2014. (Disponible en <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf>).

Queral Carbonell, A., *Obtención y aportación de la prueba electrónica*, Ginés Castellet, N., *Serie de Estudios Prácticos sobre los Medios de Prueba*, ESADE, Bosch Editor, 2011.

Rayón Ballesteros, MC., Gómez Hernández, JA., “*Ciberdelitos: Particularidades en su investigación y enjuiciamiento*”, Anuario Jurídico y Económico Escorialense, XLVII (2014).

Rodríguez Lainz, J.L., “Internet de los objetos y secreto de las comunicaciones”, Diario La Ley, nº 8034, Doctrina, 2013.

Sanchís Crespo, C., *La prueba en soporte electrónico. (Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia)*, Thomson Reuters Aranzadi, Navarra, 2012, p. 713.

Vegas Torres, J., *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*, Universidad Rey Juan Carlos, Cátedra de Investigación Financiera y Forense KPMG-URJC, Madrid, 2011.

Velasco Núñez, E., “Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías”, El Derecho, Revista de Jurisprudencia, núm. 4, 24 de febrero de 2011.

Vilasau Solana, M., *Derecho de intimidad y protección de datos personales*, Peguera Poch, M., *Derecho y nuevas tecnologías*, UOC, Barcelona, p. 93-136

RECURSOS DE INTERNET

Arévalo, M., Las mejores aplicaciones de mensajería instantánea, ABC, 11 de noviembre de 2011.

Cisco VNI Mobile 2016, “Internet y fundamentos de informática: servicios, terminología y conceptos”, INCIBE (Instituto Nacional de Ciberseguridad). <https://www.incibe.es>

Fernández Porcel, L.A., *La prueba electrónica en los juzgados*, LEXNews, 4 de febrero de 2015. <http://www.lexnews.es/la-prueba-electronica-en-los-juzgados/>