Universitat d'Alacant
Universidad de Alicante

Facultat de Dret
Facultad de Derecho

FACULTAD DE DERECHO

MÁSTER DE ACCESO A LA ABOGACÍA

TRABAJO FIN DE MÁSTER

CURSO ACADÉMICO [2020-2021]

TÍTULO:

LA PRUEBA ELECTRÓNICA EN EL PROCESO CIVIL

AUTOR:

B. ALEJANDRO RIVERA UPEGUI

TUTOR ACADÉMICO:

D. ISAAC CARLOS BERNABEU PÉREZ

Índice

I. ABREVIATURAS

- art/s.: artículo/s
- ATS: Auto del Tribunal Supremo
- CC: Real Decreto de 24 de julio de 1889, por el que se publica el Código Civil
- CE: Constitución Española de 1978
- CP: Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- DA: Disposición Adicional
- DGRN: Dirección General de los Registros y el Notariado
- EM: Exposición de Motivos
- FJ: Fundamento (o Razonamiento) Jurídico (o de Derecho)
- LAJ: Letrado de la Administración de Justicia
- LEC: Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
- LFE: Ley 59/2003, de 19 de diciembre, de Firma Electrónica (derogada)
- LO: Ley Orgánica
- LOPD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- LOPJ: Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
- LSSICE: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- RAE: Real Academia Española de la lengua
- Reglamento e-IDAS: Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
- SAP: Sentencia de la Audiencia Provincial
- ss.: siguientes
- STC: Sentencia del Tribunal Constitucional
- STS: Sentencia del Tribunal Supremo (Sala Primera, si no se indica otra cosa)
- TC: Tribunal Constitucional
- TIC: Tecnologías de la Información y la Comunicación
- VVAA: Varios Autores

II. INTRODUCCIÓN

A medida que pasan los años, los documentos tangibles se desvanecen para dar paso a los que no son, en esencia, tangibles. Esto se debe en gran medida a la globalización electrónica y al auge de los medios digitales de comunicación, es decir, a las llamadas nuevas Tecnologías de la Información y la Comunicación (en adelante, TIC), las cuales hacen posible la ruptura del espacio tiempo.

En consecuencia, casi todos los quehaceres de nuestro día a día (trabajar, formarse, entretenerse y relacionarse) se han informatizado[1], siendo muy usual que la información contenida en internet resulte, en muchas ocasiones, el único recurso o la única prueba que existe para acreditar un hecho fáctico, que coexiste en ambos mundos (el real y el digital), y que puede versar acerca de materias muy diversas, desde contractuales -actividades comerciales, despidos de trabajadores, servicios defectuosos o incumplimientos de contrato- hasta no contractuales, como los que surgen de accidentes, diversos delitos, daños, publicaciones indebidas y demás. Por ejemplo, cada vez más letrados fundamentamos nuestras pretensiones en chats intercambiados en WhatsApp, e-mails, fotografías digitales, grabaciones de voz, archivos guardados en la «nube» o en un lápiz de memoria USB (*pen drive*), etc.

Como ventaja, podemos decir que la red informática mundial (Internet) facilita el intercambio de bienes y servicios, comunicaciones y el acceso a una cantidad ingente de información. Sin embargo, como inconveniente, también diríamos que conlleva el factor potencial de que, a través de la misma, se lesionen bienes y derechos protegidos por nuestras normas jurídicas[2], por lo que es una de las mayores fuentes de prueba.

---

[1] Sobre todo en el año 2020, que ha supuesto una revolución en el mundo laboral, tanto en la Prevención de Riesgos Laborales -con el Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19-, como en el incremento del teletrabajo -a través del Real Decreto-ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria ocasionada por la COVID-19-. Asimismo, en la educación, en la que la teleformación ha pasado a ser la protagonista.

[2] Tal y como dispone, en su Considerando 6, la Directiva 2002/58/CE, de 12 de julio, relativa a la privacidad y a las comunicaciones electrónicas: "*Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a*

Por ello, ante este panorama, a los abogados no nos queda más remedio que formarnos y actualizarnos digitalmente en la práctica jurídica del derecho procesal, además de servirnos de toda la ayuda que nos puedan brindar los grandes profesionales que hay en nuestro mundillo (en concreto, me refiero a notarios y Letrados de la Administración de Justicia), así como en el de la informática (ingenieros y programadores), junto con las diferentes herramientas que se creen para ello (plataformas de servidores de confianza). De esta manera, con la colaboración de estos profesionales y de los servicios que presten las entidades especializadas en la materia, podremos llegar al objetivo que nos sea encomendado, ya sea presentar y validar en un proceso judicial una prueba electrónica (demostrar su certeza), o ya sea impugnarla e invalidarla (demostrar su manipulación o alteración) y así vislumbrar exitosa y convenientemente el camino del juzgador.

En definitiva, la finalidad de este trabajo es analizar de formar estructurada el régimen jurídico que actualmente existe para presentar como pruebas el contenido de los medios electrónicos, tanto en la legislación nacional (centrándonos en la civil), como internacional, respondiendo a una serie de interrogantes que nos surgen en estos casos. Además, hemos de resaltar la más que considerable ventaja que nos lleva, como de costumbre, la realidad de facto que hay en hay en nuestra sociedad (en este caso la digital) a la normativa vigentemente (ambigua y obsoleta), ya que nos encontramos inmersos en una era, no tan nueva, de las redes sociales (RRSS) y de la intermediación electrónica.

III. ANTECEDENTES

1. Principios de acceso de la prueba al proceso

Desde el comienzo de nuestra democracia, la Constitución, en su artículo 24.2, avalaba que toda persona inmersa en un procedimiento judicial pudiera presentar cualesquiera medios de prueba que considerase oportunos para ejercitar y acreditar su derecho de defensa, lo que se traduce al derecho de proposición de prueba y,

través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad".

consecuentemente, a que se practiquen y se valoren por un Juez o, para el caso de que se nos deniegue este derecho, a recurrir tanto su inadmisión, o falta de práctica (si se ha admitido), como su no valoración por el juzgador cuando haya sido practicada.

El silogismo judicial se compone de una premisa mayor y una premisa menor. La premisa mayor no es más ni menos que la norma jurídica de cobertura. La premisa menor se respalda de los hechos que se consideran probados y que han de subsumirse en el supuesto de hecho de la norma jurídica, y con ello, dar lugar a una conclusión. La misma se consigue acreditando hechos alegados a través de las pruebas que se consideren pertinentes.

Así, nos podemos servir de diferentes soportes para la aportación de pruebas, ya sea de la manera clásica, esto es, en papel, o bien mediante el soporte más utilizado hoy en día, es decir, el electrónico[3]. Sin embargo, a diferencia de la presentada en soporte material, de percepción directa, la estructurada en formato digital o electrónico únicamente se puede analizar su contenido por medio de un dispositivo tecnológico compatible con su lectura binaria, ya sea visual (señales ópticas) o auditiva (señales magnéticas)[4].

2. Diferencia entre fuentes y medios de prueba digitales

Las fuentes de prueba que englobamos en la denominada prueba electrónica son: las imágenes, las palabras y los sonidos, que son la realidad pasada y recogida o almacenada en los medios de prueba[5]. Por ello se dice que una fuente de prueba se diferencia de un medio probatorio por ser de naturaleza material, algo sustancial que preexiste de manera autónoma o ajena al proceso (las partes, los testigos, documentos, el objeto de enjuiciamiento, la experiencia del técnico). Por ende, se trataría de un concepto extrajurídico (o ajurídico). En cambio, los medios de prueba tienen su causa como

[3] PÉREZ PALACI, J. E.: "La prueba electrónica: Consideraciones". Universitat Oberta de Catalunya, Barcelona, 2014, pp. 3 y 4. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf

[4] GONZÁLEZ-MENESES GARCÍA-VALDECASAS, M.: *La función notarial en el medio electrónico*. Academia Matritense del Notariado, 2011, p. 47. URL: https://www.elnotario.es/images/pdf/2710201-MANUELGONZALEZMENESES.pdf.

[5] DE PRADA RODRÍGUEZ, M. y VVAA: *Nuevos horizontes del derecho procesal*. J.M. Bosch Editor. Barcelona, 2019, p. 344.

actividad que forma parte del proceso, sin el cual no existirían (los interrogatorios, pruebas documentales, el reconocimiento judicial o el dictamen de peritos)[6].

En consecuencia, medio de prueba es aquel instrumento de naturaleza procesal por el cual el juzgador llega a una conclusión sobre los hechos acaecidos en los que se fundamentan cada una de las pretensiones y alegaciones de las partes[7]. A modo de ejemplo, se podría presentar como medio electrónico que contuviese evidencias (digitales) cualquier dispositivo o soporte tecnológico, tales como móviles, ordenadores, *smartwatches*, tabletas, *pen drives*, CD's, DVD's, reproductores MP3 o MP4…[8].

Así, tecnológicamente hablando, la fuente de la prueba es la información electrónica guardada y reproducida en dispositivos electrónicos, mientras que el medio de prueba es la manera en la que ese contenido se aporta en el proceso como actividad probatoria[9].

Nuestra Ley de Enjuiciamiento Civil (en adelante, LEC) contiene a modo ejemplificativo, en su precepto 299, diferentes medios (y fuentes) de prueba[10], los cuales se pueden clasificar en tres grupos: tradicionales (o clásicos), modernos (o actuales) y

---

[6] TESONE, R., FERRER, J. y CAÑABETE, J.: "La obtención de la prueba electrónica, su acceso al proceso civil y la garantía de derechos en materia penal". Economist & Jurist. URL: https://www.economistjurist.es/articulos-juridicos-destacados/la-obtencion-de-la-prueba-electronica-su-acceso-al-proceso-civil-y-la-garantia-de-derechos-en-materia-penal/.

[7] ASENCIO MELLADO, J. Mª.: *Derecho Procesal Civil. Parte General*. Tirant lo blanch, Valencia, 2019, p. 230.

[8] DELGADO MARTÍN, J.*: Investigación tecnológica y prueba digital en todas las jurisdicciones*. Wolters Kluwer, Madrid, 2016, p 41.

[9] BANACLOCHE PALAO, J.: *Aspectos fundamentales del Derecho Procesal Penal*. La Ley, Madrid, 2011, p. 273. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p.44.

[10] Al respecto, resulta muy ilustrativa la SAP de Barcelona (Roj: SAP B 4399/2007), Sección 13, de 2 de mayo de 2007, cuando dispone que *«con la L.E.C., se regulan un conjunto de "medios de prueba" (aunque en realidad son "fuentes" de prueba) cuya característica común es la capacidad para retener palabras y/o imágenes que se desarrollaron en un momento determinado, con posibilidad de reproducirlas después, facilitándose la oralidad, la inmediación y la concentración; pero el problema que planteaban era el de su utilización, cuando no estaban previstos expresamente, en el proceso: es decir, el cauce a través del cual introducirlos en el proceso, máxime cuando el art. 24.2 C.E. constitucionalizaba el derecho -sin limitación "objetiva", salvo la licitud, pertinencia- a utilizar los medios de prueba pertinentes para la defensa y el art. 3.1 C.C. imponía la interpretación conforme a la realidad social. En un principio se acogió la tesis de la analogía con la prueba documental, el reconocimiento judicial o la pericial, que de alguna forma se "mantiene" pues la analogía con la documental se alude en la Exposición de Motivos, singularmente los "instrumentos" del art. 384 (incluso algún precepto, expresamente los regula como documentos, como el art. 812 L.E.C., entre los que pueden acceder al monitorio; o respecto de la aportación, art. 265 y ss. o las posibilidades de exhibición, arts. 329 a 334), con la pericial, como complementaria respecto de la autenticidad (art. 382 L.E.C.) o con el reconocimiento judicial (art. 382, como el "video")».*

próximos (o futuros). Así, en su apartado 1 enumera los del primer grupo: interrogatorio de parte, documentos públicos o privados, dictámenes periciales, reconocimientos judiciales y testimonios. Continua (en su apartado 2) con los modernos: reproducciones de la palabra, sonido, imágenes, operaciones y similares. Acaba, en su apartado 3, con una cláusula abierta que da cabida a servirnos en el futuro con cualquier otro medio probatorio que pudiera surgir.

Luego, el tipo de prueba que es materia de estudio se encuadraría en la actualidad en el apartado 2, ya que cuando dice "medios de reproducción de la palabra, el sonido y la imagen" (que contienen y almacenan hechos ocurridos en el pasado) se refiere exclusivamente a dispositivos multimedia, lo que engloba la característica necesaria de ser digital o informatizado[11]. Este reciente apartado (modificado en 2015[12]), tuvo su razón de ser con la irrupción de las TIC, es decir, "el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido…)"[13].

IV. LA PRUEBA ELECTRÓNICA EN LA LEC

En gran parte, la elección de la LEC se debe a que en su art. 4 se dispone que la misma es de aplicación supletoria, esto es, en defecto de disposiciones específicas, a las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, los cuales se nutren, *mutatis mutandis*, del proceso civil.

1. Concepto de prueba electrónica

Actualmente, no existe ninguna norma legislativa nacional que defina lo qué es una evidencia digital. Por el contrario, sí podemos encontrar alguna normativa que hacen

[11] La EM de la LEC asimila como prueba documental cualquier archivo digital al señalar "que la ley prevé la utilización de nuevos instrumentos probatorios que utilice nuevos, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales".
[12] Modificada por la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
[13] BELLOCH ORTÍ, C.: "Las Tecnologías de la Información y Comunicación". Universidad de Valencia, p. 1. URL: https://www.uv.es/~bellochc/pdf/pwtic1.pdf

referencia a figuras similares más concretas, tales como documento electrónico[14], medio electrónico[15], firma electrónica[16] o certificado electrónico[17]. Sin embargo, la noción de prueba electrónica es mucho más amplia, ya que dentro de ella se podrían incluir como tales las figuras anteriores[18].

De esta manera, la cuestión a tratar en este epígrafe no tiene un sentido unívoco. Prueba de ello, es que la doctrina la denomina de diversas formas, entre otras, prueba del hecho virtual, digital[19], cibernética o en soporte electrónico[20], tecnológica[21], informática[22], telemática o, simplemente, prueba electrónica[23], decantándose la mayoría por esta última.

---

[14] Por ejemplo, en la letra j) del Anexo de definiciones de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, lo define como *"información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"*.

[15] El citado Anexo de la Ley 11/2007, dispone en su letra p) sobre el medio electrónico que es aquel *"mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras"*.

[16] La letra l) del anterior Anexo -haciendo referencia a lo que establece el art. 3 de la recientemente derogada Ley 59/2003, de 19 de diciembre, de Firma Electrónica (en adelante, LFE)- dispone que es el *«conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante»*.

[17] El art. 6 LFE establecía, en su apartado 1, que el certificado electrónico *"es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad"*. Asimismo, su apartado 2 añadía que *"el firmante es la persona que utiliza un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa"*.

[18] BUENO DE MATA, F.: *Prueba electrónica y proceso 2.0*. Tirant lo blanch, Valencia, 2014, p. 95.

[19] ARMENTA DEU, T.: "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre". IDP. Revista de Internet, Derecho y Política, Universidad de Girona, 2018. URL: https://www.raco.cat/index.php/IDP/issue/view/28731/125.

[20] SANCHÍS CRESPO, C.: "La prueba en soporte electrónico", en VALERO TORRIJOS, J. (coord..), *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2001, de 5 de julio.* Thomson Reuters Aranzadi, Navarra, 2012, p. 713. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C.: *La prueba electrónica en la era digital*. Wolters Kluwer, Madrid, 2017, p. 26.

[21] ARRABAL PLATERO, P: *La prueba tecnológica: aportación, práctica y valoración*. Tirant lo blanch, Valencia, 2020.

[22] GINÉS CASTELLET, N. y ABEL LUCH, X.: *Empresa y prueba informática*. Barcelona, 2007. Obra citada por BUENO DE MATA, F., *op. cit*., p. 128

[23] OLIVA LEÓN, R., VALERO BARCELÓ, S. (Coords.) y VVAA: *La prueba electrónica. Validez y eficacia procesal.* Juristas con futuro, 2016. E-book disponible en: https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf.

Grosso modo, para dar una primera definición del sustantivo compuesto que nos incumbe, creemos conveniente primero diseccionar cada una de las palabras que lo componen.

En primer lugar, una definición propia de la prueba debe contener tres elementos: materialidad, procesalidad y subjetividad (componentes integradores de la noción de prueba judicial)[24]. Así, en derecho procesal, ASENCIO MELLADO[25] define la prueba[26] como «aquella actividad de carácter procesal cuya finalidad consiste en lograr la convicción del Juez o Tribunal acerca de la exactitud de las afirmaciones de hecho operadas por las partes en el proceso». Tal conducta activa tiene el objetivo de persuadir al juzgador cognitivamente a través de personas (testimonios) u otras cosas (documentos u otros objetos) una serie de información acerca de hechos acaecidos.

En segundo lugar, según la RAE, digital se refiere a todo dispositivo o sistema que crea, presenta, transporta o almacena información mediante la combinación de bits, siendo esta la definición que más se aproxima a lo que implica una prueba electrónica[27].

Pues bien, si hacemos una valoración conjunta de ambos conceptos, podríamos dar una primera definición de la prueba electrónica diciendo que es aquella que contiene información de valor probatorio guardada en un medio digital o transmitida por dicho medio, a la que se da el mismo tratamiento que a un documento, pero en este caso electrónico. De esta última definición podemos destacar los siguientes elementos[28]:

i) La noción de información es amplia, cabiendo en la misma cualquier clase de dato[29].

---

[24] ILLÁN FERNÁNDEZ, J.: *La prueba electrónica, eficacia y valoración en el proceso civil*. Marcial Pons, Pamplona, 2009, p. 227. Obra citada por BUENO DE MATA, F., *op cit*., p. 97.
[25] ASENCIO MELLADO, J. Mª., *op. cit*., p. 217.
[26] Por su parte, la RAE, en uno de los muchos significados que da a la palabra prueba, dispone que se trata de una "razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo".
[27] No como esta última palabra, electrónica, que según la RAE es aquello "perteneciente o relativo al electrón". Por este motivo consideramos que es más adecuado el uso del adjetivo digital, ya que su definición, como se puede comprobar, se asemeja más.
[28] DELGADO MARTÍN, J., *op. cit*., pp. 41-43.
[29] En concordancia con el art. 1.b) del Instrumento de Ratificación por España del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, que estima por datos informáticos *"cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función".*

ii) Que ha de ser producida, almacenada o transmitida por medios electrónicos.

iii) Que tiene efectos acreditativos de hechos que pueden servir a un proceso judicial de cualquier orden.

Asimismo, consideramos acertada la definición dada por BUENO DE MATA[30], quien dispone que la prueba electrónica es aquella «presentada informáticamente y que estaría compuesta por dos elementos: uno material que depende de un hardware, es decir la parte física de la prueba y visible para cualquier usuario de a pie, por ejemplo la carcasa de un Smartphone o un USB; y por otro lado un elemento intangible que es representado por un software, consistente en los metadatos y archivos electrónicos modulados a través de unas interfaces informáticas».

2. Modalidades

De la definición dada de la prueba electrónica, analizamos que concurren dos elementos fundamentales para su representación. De una parte, el físico, que se produce necesariamente por un *hardware*. De otra parte, uno lógico, que es interpretado por un *software* o programa informático[31].

Por esta razón, se pueden diferenciar dos modalidades de prueba electrónica: por un lado, los datos o informaciones acumuladas en un dispositivo, sistema o aparato tecnológico, tales como los medios de almacenamiento masivo; y, por otro lado, los transferidos por redes de comunicación abiertas o restringidas, ya sean televisivas, telefónicas (fijas o móviles), o por internet[32].

En cambio, si nos referimos al concepto abierto de documento electrónico[33] -ya que siempre que se presente una prueba electrónica habrá, directa o indirectamente, un

[30] BUENO DE MATA, F., *op. cit.*, p. 130.
[31] DE URBANO CASTRILLO, E.: *La valoración de la prueba electrónica*. Tirant lo blanch, Valencia, 2009, p. 47.
[32] ARMENTA DEU, T., *op. cit*., p. 71.
[33] La LEC permite, en su art. 135. 1, que se presenten *"escritos y documentos en formato electrónico todos los días del año durante las veinticuatro horas"*, añadiendo que, "p Presentados los escritos y documentos por medios telemáticos, se emitirá automáticamente recibo por el mismo medio, con expresión del número de entrada de registro y de la fecha y la hora de presentación, en la que se tendrán por presentados a todos los efectos. En caso de que la presentación tenga lugar en día u hora inhábil a efectos procesales conforme

documento del mismo tipo-, también encontramos dos modalidades de documentos diferentes, estos son, los públicos y los privados, que a continuación detallamos[34].

De modo que el documento electrónico público es el firmado electrónicamente por fedatario público. Dentro de esta clase podemos encontrar, a su vez, los siguientes (art. 317 LEC):

- Los librados por autoridad judicial (judiciales), tales como las resoluciones y diligencias de actuaciones judiciales, así como los testimonios que de las mismas expidan los LAJ.
- Los notariales, es decir, autorizados por notario[35]. Se produce una total equiparación de efectos jurídicos independientemente del soporte que se utilice (digital o material)[36].
- Los administrativos u oficiales expedidos por los Secretarios y funcionarios con facultad certificante de las Administraciones Públicas, en relación con los actos administrativos de éstas, entre ellos, las certificaciones de los Registradores de la Propiedad o Mercantiles y de los funcionarios facultados para dar fe en el ejercicio de sus funciones públicas[37].

---

a la ley, se entenderá efectuada el primer día y hora hábil siguiente. Continúa señalando que "a efectos de prueba y del cumplimiento de requisitos legales que exijan disponer de los documentos originales o de copias fehacientes", se remite al art. 162.3, el cual establece que *"cuando la autenticidad de resoluciones, documentos, dictámenes o informes presentados o transmitidos por los medios a que se refiere el apartado anterior sólo pudiera ser reconocida o verificada mediante su examen directo o por otros procedimientos, podrán, no obstante, ser presentados en soporte electrónico mediante imágenes digitalizadas de los mismos, en la forma prevista en los artículos 267 y 268 de esta Ley, si bien, en caso de que alguna de las partes, el tribunal en los procesos de familia, incapacidad o filiación, o el Ministerio Fiscal, así lo solicitasen, habrán de aportarse aquéllos en su soporte papel original, en el plazo o momento procesal que a tal efecto se señale"*.

[34] DELGADO MARTÍN, J., *op. cit*., pp. 58 y 59.

[35] El art. 17 bis de la Ley del Notariado de 1862 afirma que *"los instrumentos públicos a que se refiere el art. 17 de esta Ley, no perderán dicho carácter por el solo hecho de estar redactados en soporte electrónico"*, y añade, más adelante, que *"los documentos públicos autorizados por Notario en soporte electrónico, al igual que los autorizados sobre papel, gozan de fe pública y su contenido se presume veraz e íntegro de acuerdo con lo dispuesto en esta u otras leyes"*.

[36] GONZÁLEZ-MENESES GARCÍA-VALDECASAS, M.: "La función notarial en el medio electrónico". Conferencia pronunciada el 27 de octubre de 2011 en la Academia Matritense del Notariado, p. 47. URL: https://www.elnotario.es/images/pdf/2710201-MANUELGONZALEZMENESES.pdf

[37] Así, el artículo 238 de la Ley Hipotecaria consagra: *"Los libros de los Registros de la Propiedad, Mercantiles y de Bienes Muebles deberán llevarse por medios informáticos que permitan en todo momento el acceso telemático a su contenido. El Registro dispondrá de un sistema de sellado temporal que dejará constancia del momento en que el soporte papel se trasladó a soporte informático."*

Por el contrario, el documento privado electrónico sería todo aquel que no se pueda incardinar en los anteriores. Si bien, en ocasiones estos pueden gozar de alguna fuerza probatoria que haga desvirtuar lo alegado por la contraparte o traslade la carga de la prueba a la misma que impugna su autenticidad o contenido, tal y como se verá en el apartado sobre los diferentes medios de prueba.

3. Caracteres

En primer lugar, creemos conveniente analizar la principal diferencia entre la clásica prueba documental y la acreditación mediante ficheros electrónicos[38].

Así, al documento en soporte papel se le otorga las características intrínsecas de perdurabilidad e inalterabilidad (ambas relativas). De esta manera, podemos afirmar que el papel permite que los pactos queden plasmados físicamente y se mantengan en el tiempo sin que apenas sufran cambios (con unas condiciones óptimas), siendo las posibles modificaciones que se puedan producir de fácil detección y localización (más aún si gozamos de copias libradas en el momento de formalización).

En contraposición a la principal fuente de prueba clásica o tradicional, el fichero electrónico contiene una serie de metadatos que ofrecen información específica de la misma (fecha de creación o modificación)[39], es decir, "datos sobre datos". En palabras de PERALES CAÑETE[40], «todo archivo informático, por lo general, dispone de un grupo de datos "ocultos" que describen el contenido informativo de un objeto al que se denomina recurso, son los denominados metadatos».

A partir de esta diferencia fundamental, podemos relacionar una serie de características propias de las pruebas electrónicas:

- Son heterogéneas. Es de destacar la gran diversidad de hechos o métodos de investigación que pueden llevarse a cabo mediante las TIC's, lo que dificulta

[38] ANHUIANO JIMÉNEZ, J. Mª., en "La prueba electrónica en la banca digital. El soporte duradero", E-book «La prueba electrónica…», *op. cit*., pp. 71-74.
[39] ARRABAL PLATERO, P., *op. cit*., pp. 41 y ss.
[40] PERALES CAÑETE, R., en "Exiftool: ¿Los metadatos sirven de algo?", E-book «La prueba electrónica…», *op. cit*., p. 110.

la unificación de criterios procesales para su tratamiento y valoración como prueba, ya que en su obtención pueden verse afectados distintos derechos fundamentales o aportarse y practicarse por otros medios.

- Son intangibles[41]. Su esencia es virtual, ya que las evidencias electrónicas se encuentran en formatos electrónicos, pudiendo multiplicarse miles de veces, diluyéndose así las probabilidades de verificar el original de las copias. Sin embargo, partiendo de un criterio cronológico y en función de los llamados «datos de tráfico», se puede distinguir el primer documento de los sucesivos[42].

- Son volátiles. La evidencia electrónica es fácilmente manipulable[43], sin que sus modificaciones sean fácilmente detectables, pudiéndose crear pruebas electrónicas falsas *ad hoc* con el fin de obtener un fallo favorable[44]. Por esta razón es exigible una mayor prudencia ante la valoración de una prueba digital[45], debiéndose aportar un dictamen pericial informático que acredite su autenticidad cuando alguna de las partes impugne esta.

- Son delebles. Las evidencias electrónicas pueden ser fácilmente borradas, tanto de forma casual como intencional, pudiendo también destruirse los soportes físicos en los que se encuentran almacenadas (discos duros)[46]. Por ello, al ser este tipo de prueba tan vulnerable a los cambios, una buena estrategia sería adoptar medidas para su aseguramiento.

- Son mediatas. Mientras la prueba documental en soporte papel es de visualización inmediata, la electrónica requiere la intervención de un hardware

---

[41] PÉREZ PALACI, J. E., *op. cit*., p. 13.
[42] ABEL LLUCH, X. "Prueba electrónica", en *La prueba electrónica. Colección de Formación Continua Facultad de Derecho ESADE*, J. M. Bosch editor, 2011, p. 135. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 28.
[43] Así lo manifiesta la STS de 19 de mayo, Sala Segunda, de lo Penal (Roj: STS 300/2015), en su FJ 4, cuando afirma que "la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo".
[44] Sobre el delito de falsificación documental, véanse los artículos 236 y siguientes del Código Penal.
[45] No obstante, también puede modificarse cualquier documento impreso o incluso la declaración de un testigo.
[46] Acerca del delito de daños informáticos se pueden consultar los artículos 264 y siguientes del Código Penal.

y software que permita esa visualización. Así, si se aporta un pendrive con un archivo en formato PDF o JPG se requiere un ordenador, así como el programa que lo reproduzca, lo que puede llegar a ser un inconveniente a la hora de acceder a la prueba, aportarse al proceso o practicarse.

Otras características que podemos nombrar son las siguientes:

- Pueden ser parciales. A menudo, las evidencias digitales se encuentran es soportes (físicos o virtuales) que están en manos de la contraparte procesal o, incluso, de un tercero, como por ejemplo ocurre con bases de datos, emails y sistemas de almacenamiento en la nube o *cloud computing* (Google Drive, iCloud y similares).

- Pueden ser unilaterales. Las transacciones electrónicas suelen ser entre ausentes, por lo que es necesario el uso de un dispositivo informático controlado por una de ellas. Un ejemplo se da en el acceso como usuario a alguna página web, en donde quien presta los servicios es el único habilitado para acreditar o alterar lo que en ella ocurre.

- Pueden ser intrusivas[47]. En ocasiones, la recogida de evidencias digitales puede llegar a resultar una injerencia a derechos y libertades fundamentales tales como, por ejemplo, el derecho a la intimidad (art. 18.1 CE), derecho al secreto de las comunicaciones (art. 18.3 CE) o derecho a la autodeterminación informativa (art. 18.4 CE). Por ello, en la obtención de pruebas electrónicas suelen surgir cuestiones sobre su ilicitud, dando cabida a impugnaciones de difícil dilucidación.

- Pueden ser ubicuas. Otra de las notas inherentes a la prueba tecnológica es la transnacionalidad. Si bien, es cierto que no todas las evidencias digitales operan en la Red, frecuentemente sí que se desenvuelven y se obtienen de Internet. Esto conlleva una gran problemática a la hora de determinar la competencia territorial por la "deslocalización" de Internet.

[47] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 29.

- "Datos de tráfico" (huella digital). Una característica más de la prueba informática se relaciona con los rastros de información que se generan cuando se usan archivos electrónicos, es decir, los metadatos. Con ellos podemos analizar la información y comprobar las características y modificaciones de estos archivos, aportándonos datos complementarios. Estos vestigios suelen quedar grabados en archivos remotos o en el propio terminal[48].

- Media electrónica. La "media electrónica" comporta los riesgos de la generación de identidades ficticias y de usurpación de identidad derivados del anonimato o no personación física, ya que frecuentemente no podemos estar seguros de quién está detrás.

- Publicidad. Esta característica se manifiesta cuando se difunde la información probatoria por medio de la red mundial de telecomunicación llamada Internet.

V. MEDIOS PROBATORIOS ELECTRÓNICOS

Primeramente, los medios probatorios que proponemos en esta obra no son, de modo alguno, los únicos que existen, no siendo, por tanto, una enumeración cerrada[49], ya que se trata de un campo en el que se producen asiduamente numerosas modificaciones e innovaciones, dada su heterogeneidad y la ley no establece una limitación de los medios que se pretendan usar, por lo que podrán utilizarse todos aquellos que estén al alcance de los usuarios, siempre y cuando el órgano jurisdiccional disponga de los medios técnicos necesarios para su reproducción, esto es, para la práctica de la prueba electrónica (art. 384.1 LEC). De lo contrario, la parte proponente deberá aportar adecuadamente los medios tecnológicos que requiera la prueba en cuestión[50].

[48] BONACHERA VILLEGAS, R., "El registro de archivos informáticos, una cuestión necesitada de regulación", *Revista General de Derecho Procesal Iustel*, nº 27, 2012, p.2. Obra citada por ARRABAL PLATERO, P., *op. cit.*, p. 46.
[49] Al igual que realiza la LEC en su art. 229.3, que contiene un criterio de 'numerus apertus'.
[50] DELGADO MARTÍN, J., *op. cit.*, pp. 56.

Asimismo, hay que tener en cuenta que en un mismo proceso pueden presentarse y solicitarse varios medios probatorios de forma cumulativa. Un ejemplo sería la aportación de un smartphone que contiene un chat de WhatsApp, junto a su correspondiente transcripción escrita, para solicitar el cotejo del LAJ, o proponer la declaración testifical (o el interrogatorio de parte), acerca del contenido de tal conversación[51].

Por último, hemos de especificar que existen ciertos tipos de pruebas que son creadas de manera automática por máquinas, tales como los registros de sistemas de telefonía, de operaciones bancarias o de un radar de velocidad. En estos supuestos, si se requiere, será necesario acreditar que el sistema informático funcionaba y se mantenía correctamente en el momento en el que se generaron los datos[52].

1. Pruebas electrónicas con presunciones de veracidad

A. Cotejados por fedatario público

a. Acta notarial

En materia de actas notariales son de aplicación los artículos 198 y siguientes del Reglamento Notarial.

Así, según el primero de ellos, *"los notarios, previa instancia de parte* […] *extenderán y autorizarán actas en que se consignen los hechos y circunstancias que presencien o les consten y que por su naturaleza no sean materia de contrato".* Igualmente, el art. 144 del mismo texto legal prevé que *"las actas notariales tienen como contenido la constatación de hechos o la percepción que de los mismos tenga el notario, siempre que por su índole no puedan calificarse de actos y contratos, así como sus juicios o calificaciones"*.

[51] ALONSO-CUEVILLAS: "Internet y prueba civil", *Revista Jurídica de Catalunya*, núm. 4, 2001, p. 1078. Obra citada por DELGADO MARTÍN, J., *op. cit*., p. 53.
[52] VAN DEN EYNE, A.: "Retos relacionados con la prueba electrónica (parte I)". Disponible en: https://eynde.es/es/retos-relacionados-con-la-prueba-electronica-parte-i/

Por tanto, a diferencia de los documentos notariales (escrituras y pólizas de contratos o manifestaciones de voluntad), el objeto del acta notarial son los hechos, lo que significa que el Notario en las actas da fe únicamente de lo que percibe y le muestran, convirtiéndose las mismas en pruebas preconstituidas de hechos que podrán ser alegados posteriormente en diferentes ámbitos (judicial, administrativo o privado), no importando entonces si esos hechos han desaparecido o no se reiteran más[53].

En nuestra sede, añade el apartado 2 de este artículo, relativo al acta de archivos informáticos, que *"cuando un notario sea requerido para dejar constancia de cualquier hecho relacionado con un archivo informático, no será necesaria la transcripción del contenido de éste en soporte papel, bastando con que en el acta se indique el nombre del archivo y la identificación del mismo con arreglo a las normas técnicas dictadas por el Ministerio de Justicia. Las copias que se expidan del acta deberán reproducir únicamente la parte escrita de la matriz, adjuntándose una copia en soporte informático no alterable según los medios tecnológicos adecuados del archivo relacionado. La Dirección General de los Registros y del Notariado, de conformidad con el artículo 113.2 de la Ley 24/2001, de 27 de diciembre, determinará los soportes en que deba realizarse el almacenamiento, y la periodicidad con la que su contenido debe ser trasladado a un soporte nuevo, tecnológicamente adecuado, que garantice en todo momento su conservación y lectura"*.

Este artículo sería muy relevante de cumplirse los mandamientos que dirige a la propia Administración, ya que a día de hoy ni la DGRN ni el Ministerio de Justicia ha determinado ninguna de estas normas, lo cual cada vez se hace más necesario[54].

No obstante lo anterior, el notario GONZÁLEZ-MENESES[55], destaca que el art. 114.1 de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, bajo la rúbrica "Constatación fehaciente de hechos relacionados con soportes informáticos", permite identificar un determinado archivo informático respecto del cual se pretende constatar fehacientemente su existencia y contenido, sin necesidad

[53] "Actas notariales". *Consejo General del Notariado*. Consultado el 6 de enero de 2021 en el siguiente enlace: https://www.notariado.org/portal/actas-notariales
[54] ROSALES DE SALAMANCA RODRÍGUEZ, F.: "Validez y eficacia procesal de las evidencias digitales", en *La Prueba Electrónica…op. cit*., p.
[55] GONZÁLEZ-MENESES GARCÍA-VALDECASAS, M., *op. cit*., pp. 54 y ss.

de protocolizar una copia impresa en papel del mismo[56], bastando con que se reseñe en el documento notarial el *hash*[57] o huella digital. El referido autor describe el proceso de la siguiente manera: Si al tiempo de recibirse el depósito el notario obtiene el *hash* de todo el contenido de un soporte electrónico (CD-ROM, USB…), basta con protocolizar ese *hash* para tener perfectamente identificado el contenido del soporte y, así, tener la certeza de que en cualquier momento y por cualquiera se podrá verificar que las posteriores reproducciones de la información contenida en el soporte en cuestión no ha sido alterada (asegurándose con ello la correspondiente cadena de custodia).

Por otro lado, el artículo 199.2 impide que el Notario de fe de hechos que requieran conocimientos periciales. Así, el notario únicamente podrá constatar de manera limitada lo que presencie o perciba a simple vista, en los detalles que el cliente le requiera -tales como el contenido, la fecha, hora, la dirección del dominio, etc. (lo que bien podría estar previamente alterado por el mismo requirente o un tercero)-, no pudiendo, por tanto, pronunciarse acerca de aquello que requiera conocimientos especializados en informática, como por ejemplo emitir juicios de valor acerca de una posible alteración y similares circunstancias (a no ser que el mismo Notario fuera también titulado en esta materia).

b. El cotejo del Letrado de la Administración de Justicia

La LEC habilita continuamente al LAJ a que de fe de la exactitud de las copias de los documentos que se presentan en un proceso judicial. Como ejemplo, podemos mencionar el previsto en el art 333 para la extracción de copias de documentos que no sean textos escritos. Así, este artículo dispone que cuando se trate de dibujos,

---

[56] La aludida disposición establece que: […] *cuando un notario sea requerido para dejar constancia de cualquier hecho relacionado con un archivo informático, no será necesaria la transcripción de su contenido en el documento en soporte papel, bastando con que en éste se indique el nombre del archivo y una función alfanumérica que lo identifique de manera inequívoca […]. Las copias que se expidan del documento confeccionado podrán reproducir únicamente la parte escrita de la matriz, adjuntando una copia en soporte informático adecuado del archivo relacionado, amparada por la firma electrónica avanzada del notario".*

[57] *Hash* se puede describir como algoritmo o cadena alfanumérica de longitud normalmente fija (entre 20 y 50 caracteres hexadecimales) obtenida como salida de una función *hash*. Estas funciones unidireccionales, también llamadas de digest, generan un resumen de la información de entrada, de modo que tal salida sólo puede ser producida por esa entrada y ninguna otra. Se utilizan para lograr integridad de datos, almacenar contraseñas o firmar digitalmente documentos (son muy utilizados en las transacciones 'Blockchain'). Para más información véase el siguiente enlace: https://www.welivesecurity.com/la-es/glosario/#glossary-66

fotografías… y otros documentos que no incorporen predominantemente textos escritos, si sólo existiese el original, la parte podrá solicitar que en la exhibición se obtenga copia, a presencia del Letrado de la Administración de Justicia, que dará fe de ser fiel y exacta reproducción del original, haciendo referencia expresa al caso de que se presenten estos electrónicamente cuando dispone que *"si estos documentos se aportan de forma electrónica, las copias realizadas por medios electrónicos por la oficina judicial tendrán la consideración de copias auténticas"*, obteniendo de esta manera tales documentos públicos una presunción de veracidad que solo podría destruirse con una minuciosa pericia.

c. El reconocimiento judicial

El artículo 353 dispone que "el reconocimiento judicial se acordará cuando para el esclarecimiento y apreciación de los hechos sea necesario o conveniente que el tribunal examine por sí mismo algún lugar, objeto o persona", siendo por ello un medio adecuado para incorporar una prueba electrónica al proceso.

De suerte que, de oficio o a instancias de parte, el Juez puede examinar directamente por sí mismo[58]:

- El contenido del dispositivo electrónico aportado accediendo a este.
- El contenido de Internet (navegación por la red o la llamada «cibernavegación judicial»[59]) para contrastar la realidad de los hechos alegados por la parte interesada, dado que una página web puede ser considerada un "lugar" (virtual) o también un objeto[60]. Si bien, es posible que cuando se practique esta prueba, la página en cuestión ya no refleje el estado de cosas que interese en el procedimiento[61].

[58] DELGADO MARTÍN, J., *op. cit.*, pp. 75 y 76.
[59] ABEL LLUCH, X.: "¿Puede acceder el contenido de un e-mail o de una página web al proceso a través de la prueba de reconocimiento judicial?", en «Preguntas con respuestas: la prueba a consulta», *Diario LA LEY*, n.º 7564, Sección Práctica Forense, Año XXXII, Ref. D-57. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 75.
[60] ALONSO-CUEVILLAS, J.: "Internet y prueba civil", *Revista Jurídica de Catalunya*, núm. 4, 2001, p. 144. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 75.
[61] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 47.

La LEC prevé que el reconocimiento judicial pueda practicarse de forma autónoma (individual) o complementariamente con otros medios probatorios (si se propusieron a instancias de parte), tales como, la prueba pericial (art. 356 LEC) o el interrogatorio de parte y la declaración testifical (art. 357 LEC).

Si el reconocimiento judicial se practica simultáneamente con la prueba pericial, podrá realizarse al mismo tiempo que el órgano judicial navega por la red o percibe la pantalla del dispositivo en cuestión, mientras que el perito le aporta comentarios de máximas de la experiencia técnicas. Si se practicare conjuntamente con el interrogatorio de parte o declaraciones testificales, se hará de forma sucesiva, de modo que primero se procederá a navegar por la red o el aparato presente y acto seguido se tomará declaración de la parte y testigos[62].

B. Autentificados por otros instrumentos

a. Dictámenes periciales

Tanto por la vía del art. 340 y ss. LEC, en cuanto a la pericial judicial, como por el art. 384.2 LEC, para aclarar el contenido del dictamen presentado por un parte, el empleo de la pericial informática puede resultar determinante en la probática electrónica, sobre todo, si no queremos hacer depender la tutela judicial, en cada caso, del conocimiento privado del órgano judicial, ya que las reglas de la sana crítica solo deberían entrar en juego cuando un especialista ha explicado previamente lo relacionado con el *hardware* y *software* implicados en un determinado asunto[63].

Podemos definir la prueba pericial como aquel medio probatorio de carácter personal previsto expresamente en el art. 340 LEC y que consiste en que una persona (perito) especializada en una determinada materia está en una posición adecuada para aportar conocimientos científicos, artísticos, técnicos o prácticos que el Juez o Tribunal no posee cuando éstos resultan necesarios para acreditar hechos o circunstancias relevantes para el caso objeto de enjuiciamiento y con ello poder valorar adecuadamente

[62] ABEL LLUCH, X.: "Puede acceder el contenido de un e-mail…". Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 75.
[63] DE URBANO CASTRILLO, E., *op. cit.*, pp. 69 y 70.

el objeto de la pericia para consecuentemente emitir un dictamen sobre los mismos de manera precisa y segura[64].

El artículo indicado dispone en su primer apartado que "los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias". Por tanto, se prevé una dualidad de peritos, eligiéndose preferentemente el "perito titulado" -o perceptivamente si es nombrado por el Juez- y subsidiariamente al "perito entendido" o no titulado, siempre y cuando la materia en cuestión pueda encuadrarse dentro de una titulación oficial[65].

Así, en la llamada pericial informática, descartaríamos la pericial del "entendido" ya que, en una materia como la nuestra, es primordial que la misma sea realizada por un titulado y experimentado ingeniero o programador informático, para poder así ilustrar adecuadamente al juzgador, constatando con su pericia todas o algunas de las dudas que le puedan surgir, mediante el análisis de los datos o componentes de un dispositivo o red digital[66].

Este tipo de pericias se requieren, por ejemplo, cuando no se tienen los conocimientos necesarios para acceder a la información de un determinado dispositivo, debido a que sus archivos han podido ser ocultados, encriptados o eliminados. Igualmente, servirá para complementar o acreditar la información (fechas de creación, modificación o eliminación, origen y destino…) autenticidad e integridad del contenido de la información o, por el contrario, para desvirtuar tales características.

Además, en este tipo de es muy importante que se garantice y documente debidamente la respectiva «cadena de custodia», esto es siguiendo a DELGADO MARTÍN, el procedimiento que permite constatar la identidad, integridad y autenticidad

---

[64] LLOPIS BENLLOCH, J. C.: "Prueba electrónica y notariado" en *La Prueba Electrónica… op. cit*., p. 21.
[65] ABEL LLUCH, X.: "Pericial informática" en *La prueba civil a debate judicial. Estudios prácticos sobre prueba civil I*. Wolters Kluwer, Madrid, 2018, p. 186.
[66] DELGADO MARTÍN, J., *op. cit*., pp. 65 y ss.

de los vestigios o indicios de un hecho relevante para el asunto, desde que son hallados hasta que se aportan al proceso como pruebas.

Para ello es conveniente el respeto de las fases que tiene un análisis pericial informático[67]. Por un lado, desde una proyección técnica son: 1º Preservación; 2º Adquisición; 3º Análisis; 4º Documentación; 5º Presentación. Por otro lado, sobre la base de una perspectiva jurídica, de acuerdo con los diferentes momentos procesales, la pericial realizada en un dispositivo electrónico tiene las siguientes fases: i) Obtención de los datos (acceso al contenido virtual del dispositivo); ii) Clonación de los datos y cálculos del hash; iii) Elaboración del dictamen pericial al Tribunal; iv) Valoración por el Tribunal.

Así, el desarrollo del procedimiento pericial consistirá en "preservar" las evidencias digitales que se contengan en el archivo electrónico que se pretende aportan a un juicio. Está preservación se obtendrá mediante copias forenses "exactas" de la información digital almacenada que generará un código alfanumérico de la información (código *hash*). Está copia se realizará por duplicado, depositando una de ella ante Notario, y la segunda se dejará en poder del mismo perito para su posterior análisis técnico. La técnica de elección será de carácter selectivo (solo se analizará la información necesaria) realizando búsquedas "ciegas", evitando injerir en contenido que pueda ser íntimo o privado de su propietario.

Ulteriormente, los resultados de la investigación se trasladarán a un informe pericial técnico que se aportará al proceso, siendo lo habitual, que el perito acuda a juicio para ratificarse en su informe y evitar con ello posibles impugnaciones de la parte contraria[68].

En realidad, estas pericias no difieren mucho de otros tipos de pruebas periciales. Por ejemplo, un perito de accidentes puede no saber el alcance que ha tenido determinado tipo de colisión en los daños personales de los intervinientes, o un perito mecánico puede que no conozca qué elemento ha provocado los daños del vehículo que analiza[69]. Por

[67] INCIBE, "Fundamentos de un análisis forense informático", actividad de formación de Jueces y Magistrados, León, 2016. Obra citada por DELGADO MARTÍN, J., *op. cit*., pp. 70.
[68] ROJAS ROSCO, R.: "La prueba digital en el ámbito laboral ¿son válidos los "pantallazos"? en *La prueba electrónica…op. cit.*, p. 95
[69] ARRABAL PLATERO, P., *op. cit.*, p. 47.

tanto, al igual que estas, el dictamen pericial informático será valorado según las reglas de la sana crítica (art. 348 LEC).

b. Firma electrónica

En palabras de DELGADO MARTÍN, una firma electrónica constituye un mecanismo criptográfico que posibilita al receptor de un documento informático firmado digitalmente conocer la identidad del sujeto creador de dicho documento (autenticación de origen y no repudio) y asegurarse de que el contenido del mismo no ha sido alterado desde que es rubricado hasta llegar a su destino[70].

Con la publicación[71] y entrada en vigor de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, queda derogada la LFE y se adapta la normativa española al Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, Reglamento e-IDAS)[72].

Este Reglamento define en su artículo 3 (apartados 10 a 11, respectivamente), los tres tipos de firma electrónica: básica (o simple), avanzada y cualificada (o reconocida).

i. Así, la **firma electrónica básica** (no avanzada) trata de los datos en formato electrónico (por ejemplo, los metadatos) anejos o asociados a otros datos de manera electrónica que utiliza el suscritor para identificarse (firmar)[73].
ii. La **firma electrónica avanzada** es aquella que cumple con los requisitos del art. 26 del Reglamento e-IDAS, es decir, identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, estar vinculada a éste de

[70] DELGADO MARTÍN, J., *op. cit.*, p. 90.
[71] Con fecha 12 de noviembre de 2020.
[72] Este Reglamento deroga la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 (por la que se establecía un marco comunitario para la firma electrónica) y establece normas para los servicios de confianza, en particular para las transacciones electrónicas, así como un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web [art. 1, apartados b) y c)].
[73] El apartado 1 del art. 25 Reglamento e-IDAS dispone que *"no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada".*

manera única, y a los datos a que se refiere, y ser creada por medios que el firmante puede utilizar con un alto nivel de confianza y bajo su exclusivo control[74].

Esta se crea mediante una clave criptográfica (algoritmos asimétricos) que unívocamente se relaciona con el firmante de manera individualizada para cada documento. Este tipo de firma utiliza una dualidad de claves, las cuales podemos llamar cifrante y descifrante, ya que lo que se cifra con una solo se puede descifrar con la otra.

Así, con la primera se crea de manera privada y univoca la clave personal del firmante y con la segunda se reconoce una clave pública por la que se puede obtener un resumen correspondiente al documento firmado electrónicamente[75].

iii. Una **firma electrónica reconocida** es la misma que la anterior con el añadido de estar basada en un certificado reconocido que se genera mediante un dispositivo seguro de creación de firmas electrónicas[76].

A diferencia de la firma manuscrita, que es una manifestación gráfica -tanto analógica como digital[77]- del consentimiento, la firma electrónica es una forma de identificación virtual, por tanto, al amparo de esta última no se puede presuponer que el sujeto que haga uso de la misma tenga la suficiente capacidad para firmar, ni tampoco que no existan vicios en su consentimiento[78] y, consecuentemente, sea válido el negocio[79].

---

[74] Hemos utilizado la definición realizada en el artículo 3 de la derogada LFE, por su acierto e ilustración.
[75] DELGADO MARTÍN, J., *op. cit*., p. 92.
[76] Según el art. 25.3 Reglamento e-IDAS, la *"firma a electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros".*
[77] Como, por ejemplo, las que realizamos con un lápiz electrónico (o con el dedo) dentro de una pantalla táctil que nos proporciona una entidad comercial.
[78] El Reglamento e-IDAS dispone, en su artículo 2.3, que lo dispuesto en el mismo "no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma", por lo que la perfección y validez del contrato se somete a la teoría general del negocio jurídico.
[79] ROSALES, F.: "Un Notario hablando de firma electrónica". URL: https://www.notariofranciscorosales.com/un-notario-hablando-de-firma-electronica/

En cualquier caso, para que la firma electrónica avanzada tenga los efectos jurídicos que estable el art. 25.2 Reglamento e-IDAS, esto es, su equivalencia a la firma manuscrita (en cualquier Estado miembro), es necesario que esta sea librada por prestadores cualificados de servicios electrónicos que se encuentren inmersos en las listas de confianza a las que hace referencia el art. 22 del citado Reglamento, por ejemplo, la Dirección General de la Policía (respecto al DNI electrónico), la Fábrica Nacional de Moneda y Timbre (en relación con la Certificación Digital), el Consejo General de la Abogacía Española (para la firma electrónica ACA)…

Actualmente este es el método electrónico más fiable para identificar con certeza el autor que suscribe un archivo electrónico, ya que la misma añade una serie de información específica sobre la persona que rubrica un escrito[80].

Además, las garantías para apreciar una firma electrónica son superiores al cotejo de un perito caligráfico sobre una firma manuscrita, pues aquella sólo requiere unas comprobaciones técnicas, es decir, objetivas, mientras que la segunda es más sencilla de falsificar y su comprobación pericial implica unos juicios de valor y, por tanto, subjetivos, emitidos por el técnico en su dictamen. Si bien, es cierto que cabe la posibilidad de que la firma electrónica sea sustraída o entregada a un tercero, ya sea por su titular, o bien por suplantación de identidad o incluso por un error, pero esto es mucho menos probable.

Por otro lado, nos encontramos con los sellos electrónicos, que únicamente se diferencian de las firmas electrónicas en que están previstas para las personas jurídicas[81], por lo que su régimen jurídico es el mismo[82].

Por último, destacar que desde la entrada en vigencia del Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia, es obligatoria la utilización de este sistema electrónico para la presentación de escritos, su traslado y la realización de actos de comunicación, tanto por los Juzgados, Tribunales

[80] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 41.
[81] Si bien es cierto que el Reglamento e-IDAS, en su considerando 65, dispone que los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, lo cual no prevé en la firma electrónica.
[82] ROSALES, F.: "Notarios digitales, servicios y terceros de confianza". URL: https://www.notariofranciscorosales.com/notarios-digitales-servicios-y-terceros-de-confianza/

y Fiscalías como por los profesionales que colaboran con la Justicia (procuradores, abogados, peritos…), los cuales habrán de firmar digitalmente sus escritos[83].

c. Servicios de confianza

Los «servicios de confianza» se definen en el apartado 16 del 3 artículo Reglamento e-IDAS, como aquellas prestaciones electrónicas que consisten en la creación, verificación, validación y preservación de firmas, sellos o certificados electrónicos, servicios de entrega electrónica certificada y certificados para la autenticación de sitios web.

El propio Reglamento introduce en su considerando 22 una vinculación directa con la prueba electrónica, al señalar que *"para contribuir al uso transfronterizo general de los servicios de confianza, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los Estados miembros.* Si bien, precisa que *corresponde al Derecho nacional definir los efectos jurídicos de los servicios de confianza, salvo disposición contraria del presente Reglamento*[84].

Asimismo, distingue dos tipos de prestadores de servicios de confianza: los cualificados (apartado 17) y los no cualificados (apartado 18). Los primeros se diferencian de los segundos en que han de ser auditados al menos cada 24 meses -por estar sujetos a la supervisión continua del organismo de evaluación de conformidad que haya concedido tal cualificación[85]- y en que prestan un servicio de confianza que cumple con lo establecido en el art. 24 del referido Reglamento.

---

[83] En virtud de los art. 273.4 LEC: "La presentación se realizará empleando firma electrónica reconocida y se adaptará a lo establecido en 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"; y del art. 31 LEC, que establece que "los litigantes serán dirigidos por abogados habilitados para ejercer su profesión en el tribunal que conozca del asunto. No podrá proveerse a ninguna solicitud que no lleve la firma de abogado".

[84] ALAMILLO DOMINGO, I., en "Los servicios de confianza y la prueba electrónica", E-book «La prueba electrónica…», *op. cit.*, pp. 147 y 148.

[85] El artículo 17 del Reglamento e-IDAS establece que cada estado miembro fijará un organismo de supervisión de los servicios de confianza, siendo este actualmente en España el Ministerio de Asuntos Económicos y Transformación Digital (arts. 14 y ss. Ley 6/2020), así como la «etiqueta de confianza UE» para aquellos prestadores cualificados de servicios de confianza que hayan obtenido la cualificación del art. 21.2, 2º del referido Reglamento.

Así, cuando un documento electrónico está firmado mediante un certificado reconocido y seguro[86], expedido por uno de los llamados "servicios de confianza cualificados" -como lo es, por ejemplo, la firma electrónica avanzada-, su contenido gozará de una presunción de veracidad *iuris tamtun* y, según el art. 3.2 (segundo inciso) de la citada Ley 6/2020, ya que tiene unos efectos similares a los del documento privado «reconocido legalmente»[87]. Por tanto, aunque se impugnase la autenticidad de su contenido, en conformidad con el art. 326.4 LEC, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente, eso sí, siempre y cuando este servidor figurase en la lista de confianza de prestadores y servicios cualificados en el momento relevante a los efectos de la discrepancia, recayendo la carga de la desvirtuación sobre el impugnante. Asimismo, le sanciona con la asunción de las costas que se generen cuando el resultado de las comprobaciones no prospere, pudiéndole imponer, además, una multa entre 300 y 1200 euros cuando se apreciare temeridad en la impugnación.

Por el contrario, cuando se hubiese utilizado un servicio de confianza no cualificado, el documento electrónico resultante tendrá el mismo tratamiento que un simple documento privado, sin que goce, por tanto, de presunción de veracidad a su favor (aparatado 3 del art. 326 LEC). Por ello, cuando se impugne su autenticidad, recaerá la carga de la prueba sobre la parte que lo haya presentado y, por tanto, tendrá que presentar la certificación de su firma para proceder a su cotejo pericial o judicial, o cualquier otro medio de prueba útil y pertinente (art. 326.2 LEC). Si se acaba verificando su autenticidad, las costas serán a cargo del impugnante, pudiéndole, además, sancionar coercitivamente con una multa de 120 a 600, si esta hubiese sido temeraria a criterio del juzgador o tribunal (art. 320.3 LEC). En el caso de que no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el juzgador o tribunal lo valorará de conformidad con las reglas de la sana crítica (art. 326.2, II *in fine* LEC).

[86] Ya sea mediante sistemas reconocidos como Cl@ve PIN, Cl@ve Permanente, certificado digital o DNI electrónico; o ya sea mediante otros medios no tan seguros en los que para inscribirnos hemos de dar una identidad como usuario.
[87] GONZÁLEZ-MENESES GARCÍA-VALDECASAS, M., *op. cit.*, p. 47.

d. Terceros de confianza

La figura del tercero de confianza se origina ante la falta de confianza existente en las relaciones jurídico-contractuales y telemáticas que tienen las partes intervinientes para que reciba, custodie y ponga fecha a dicha prueba[88]. Así, podemos decir que es un sujeto ajeno a los obligados de una transacción electrónica al que le confían de mutuo acuerdo el archivo en soporte informático de las declaraciones de voluntad que conforman su oferta y su demanda en el seno de una contratación electrónica.

La definición de Tercero de confianza se encontraba en el art. 25[89] de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE, por sus iniciales), actualmente derogado por la reciente Ley 6/2020 -como dice su EM- "debido a que los servicios ofrecidos por este tipo de proveedores se encuentran subsumidos en los tipos regulados por el Reglamento (UE) 910/2014, fundamentalmente en los servicios de entrega electrónica certificada y de conservación de firmas y sellos electrónicos".

De la definición que nos daba dicho artículo, podemos extraer las siguientes conclusiones[90]:

- El tercero de confianza es el que se presenta por ambas partes, no únicamente por una de ellas (a diferencia de los prestadores de servicios de confianza, a los que se puede acudir unilateralmente).

---

[88] LLOPIS, J. C: "Los terceros de confianza y los notarios ¿son lo mismo?" Recuperado de: http://www.notariallopis.es/blog/i/1319/73/los-terceros-de-confianza-y-los-notarios-son-lo-mismo. Blog citado por GASTÓN E. BIELLI.: "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática". URL: http://e-procesal.com/dterceros-de-confianza-y-certificacion-de-prueba-electronica-una-nueva-frontera-en-materia-de-probatica-2109#_ftn5

[89] Este obsoleto art. disponía:

1. Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.

2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años.

[90] ROSALES, F.: "Diferencias entre un Notario y el tercero de confianza". URL: https://www.notariofranciscorosales.com/diferencias-entre-un-notario-y-el-tercero-de-confianza/

- Se limita a archivador documentos electrónicos, sin entrar a comprobar su validez ni la identidad de las partes (al contrario que los prestadores de servicios de confianza).
- El archivo del documento electrónico es temporal.
- No sustituye ni altera las funciones del notario, que bien puede éste prestar los mismos servicios con la ventaja que supone la fe pública de la que dispone.
- Los documentos electrónicos custodiados por terceros de confianza, a efectos legales, son documentos privados y, por lo tanto, no tienen ninguna presunción de validez ni carácter ejecutivo (arts. 317, 319 y 517 LEC, a sensu contrario) ni tampoco producen la entrega de la cosa objeto del contrato (art. 1462 CC).
- El tercero de confianza no elabora el documento que archiva (son las partes las que lo hacen).

Por tanto, podemos concluir que el tercero de confianza es un mero depositario "virtual" que custodia documentos electrónicos en los que consigna fecha y hora a efectos de que se mantengan inalterables los datos que constan en dichos documentos, sin que puedan realizar otras funciones como, por ejemplo, notificar fehacientemente[91] (para ello necesitarán acudir a un servicio de confianza).

Esta figura es actualmente ignorada por el Reglamento e-IDAS 910/2014, por lo que pierde prácticamente toda su razón de ser, al ser desplazados completamente por los prestadores de servicios de confianza (tanto cualificados como no cualificados).

Además, el problema que tienen este tipo de operadores de servicios es que dependen de los servicios de confianza cualificados para la verificación fehaciente de operaciones tales como la verificación de la identidad de las partes, por lo que si no hacen uso de los sistemas de sus mecanismos de seguridad (como la firma electrónica) su valor probatorio es muy cuestionable, ya que ni se verificaría la identidad de las partes ni tampoco la autenticidad o legalidad del documento que se le entrega (debido a que no son juristas), quedando por tanto su papel 'reductio ad absurdum'. En estos casos, únicamente

[91] La Resolución de 2 de enero de 2019, de la Dirección General de los Registros y del Notariado, en el recurso interpuesto contra la negativa del registrador mercantil y de bienes muebles XI de Barcelona a inscribir determinados acuerdos adoptados por la junta general de una sociedad, rechaza tal valor a la convocatoria efectuada por el operador "Logalty Servicios de Terceros de Confianza, S.L.".

se podría presumir (con buena fe) que los documentos que les han sido depositados se han mantenido inalterados desde la fecha de entrega (fecha que sin un sello de tiempo o *timestamp* también podría ser cuestionada).

e. Sello de tiempo electrónico

El Reglamento e-IDAS define el sello de tiempo electrónico o *timestamping* como aquellos datos electrónicos que se vinculan detalladamente con la fecha y hora de un determinado momento a un documento electrónico (facturas, recibos, encargos, contratos…) para acreditar que éste existía tal y como se presenta en el instante en el que se registra el sello [art. 3. 33)].

Los efectos jurídicos de los sellos de tiempo electrónicos se prevén en el artículo 41 del mismo texto legal. Así, en su apartado 1, dispone que "*no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico"*. Asimismo, (apartado 2) "*disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas"*. Termina este artículo estableciendo que los sellos cualificados de tiempo electrónico emitidos en un Estado miembro se reconocerán igualmente como cualificados en los demás Estados miembros.

Para cumplir la finalidad de garantizar la confianza en las operaciones comerciales y administrativas, el sellado de tiempo electrónico es proporcionado por un tercero de confianza, conocido como Autoridad de Sellado de Tiempo (TSA, por sus siglas en inglés), asegurándose con ello la integridad de las evidencias electrónicas[92].

f. Blockchain

La tecnología *blockchain* tiene un gran impacto en el mundo jurídico conforme avanzan las TIC. Sin embargo, en la actualidad no contamos a nivel nacional, ni tampoco a nivel europeo, de una normativa que regule esta red descentralizada, a diferencia de la

[92] Patricia NUÑO: "¿Qué es el sellado de tiempo?", *Ivnosys*. URL: https://www.ivnosys.com/es/que-es-sellado-de-tiempo/

mayoría de plataformas centralizadas (como Google o Facebook). Esta tecnología se utiliza sobre todo como base para las criptomonedas o monedas digitales (como el Bitcoin), pero su uso va más allá, por ejemplo, es dónde se crean y ejecutan los *Smart-Contracts* o contratos inteligentes[93].

Traducido al español sería una cadena de bloques, no obstante, se trata de una especie de base de datos especial[94] de registro inalterable, descentralizado, consensuado y distribuido en varios nodos concatenados de una red[95] P2P4, en la que se inscriben y almacenan procedimientos codificados que acreditan la existencia de eventos acaecidos en ella (prueba de cotejo), validando por sí misma la información al ser inalterable. En cada bloque se almacena:

- una cantidad de registros o transacciones válidas,
- información referente a ese bloque,
- su vinculación con el bloque anterior y el bloque siguiente a través del *hash* de cada bloque, esto es, un código único que sería como la huella digital del bloque.

Sus principales ventajas son la trazabilidad (el registro de todos los datos), la perpetuidad (grabado de datos permanente) y la inmutabilidad (inalterabilidad de los datos) de las transacciones, ya que cada bloque tiene un lugar específico e inamovible dentro de la cadena, al contener cada uno la información del *hash* del bloque anterior. La cadena completa se guarda en cada nodo de la red que conforma la *blockchain*, por lo que se almacena una copia exacta de la cadena en los demás participantes de la red. De esta manera, la información almacenada jamás se perderá, modificará o eliminará.

---

[93] Se trata de contratos que se ejecutan por sí mismos, sin la intervención de terceros, y se escriben como un programa informático en lugar de utilizar un documento impreso con lenguaje legal. Para más información sobre los *Smart-contracts* abrase el siguiente enlace: https://www.bbva.com/es/smart-contracts-los-contratos-basados-blockchain-no-necesitan-abogados/

[94] Así lo define Eva Hernández Ramos, autora del Podcast: "Conflicto entre la tecnología blockchain y la normativa de protección de datos". *Economist&Jurist*. Disponible en: https://www.economistjurist.es/articulos-juridicos-destacados/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos-2/

[95] PASTORINO, CECILIA: "Blockchain: qué es, cómo funciona y cómo se está usando en el mercado". *Welivesecurity*. Consultado el 13 de enero de 2020 en el siguiente enlace: https://www.economistjurist.es/articulos-juridicos-destacados/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos-2/

Además, cada nodo de la red utiliza certificados y firmas digitales para verificar la información y validar las transacciones y los datos almacenados en la blockchain, lo que permite asegurar la autenticidad de dicha información.

Esta plataforma puede servir, por ejemplo, para cotejar una prueba de modo directo (sin intermediarios), ya que graba la matriz de un documento (por ejemplo, un contrato, escritura o un bien digital), almacenándolo en diferentes bloques o nodos que conforman la red, de manera que, si uno de ellos modifica el documento, su vinculación con los restantes se rompe -al estar matemáticamente vinculados-, saltando una alarma al surgir en ellos una divergencia. Esto se traduce, en seguridad para el usuario, ya que inmediatamente puede saber si ha habido una modificación, al garantizarse la disponibilidad de la información en todo momento.

En definitiva, esta tecnología permite verificar, validar, rastrear y almacenar todo tipo de pruebas, como certificados digitales, servicios de logística y mensajería, contratos inteligentes y, como no, transacciones financieras.

g. Notificación electrónica certificada

Aquí hacemos mención a los emails certificados, BuroSms y burofaxes online, entre otros. Este tipo de notificaciones certificadas implican que la identidad del emisor, el contenido de la comunicación, la fecha y hora de envío, así como la fecha y hora de recibo por el destinatario queda certificada de manera fehaciente (acuse de recibo o recibí)[96]. Además, conllevan la ventaja de que su envío es instantáneo, su destinatario lo recibirá en cualquier lugar y a cualquier hora, por lo que supone un verdadero ahorro de tiempo y dinero, ya que sus precios son más económicos[97].

La definición de «servicio de entrega electrónica certificada» se encuentra en el art. 3.16 del Reglamento e-IDAS. Así, dispone que se trata de *"un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas*

[96] En el caso de los e-mails certificados y BuroSMS el destinatario que lee o recibe el mensaje no queda identificado fehacientemente, a diferencia de los Burofaxes electrónicos o postales. Para más información al respecto, véase el siguiente contenido: https://www.notificados.com/publico/emailcertificado.aspx

[97] "¿Qué es un email certificado?", *Digitel TS* [Consultado el 10/01/21]. Disponible en: https://digitelts.es/que-es-un-email-certificado

relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada".

Asimismo, los efectos jurídicos de tales servicios se prevén en el art. 43 Reglamento e-IDAS. Este artículo, en su apartado uno, determina que no se le denegarán efectos jurídicos ni admisibilidad como prueba a los datos enviados y recibidos mediante servicios de entrega electrónica certificada por el mero hecho de que estén en ese formato o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada. Sin embargo, si cumplen tales requisitos, añade el apartado 2, que el contenido y la información certificada contará con una presunción de veracidad, en concreto sobre su integridad y exactitud, del contenido e información anexa reflejada en el PDF certificado y firmado digitalmente[98] que nos envíe el servicio cualificado de entrega electrónica.

Por tanto, para hacer uso de este tipo de envíos deberemos acudir a un prestador cualificado de servicios de confianza[99] que (art. 44 Reglamento e-IDAS): identifique debidamente al remitente; garantice la identificación del destinatario antes de la entrega de los datos; proteja el envío y recepción de datos con una firma electrónica avanzada o un sello electrónico avanzado que impida la posibilidad de que modificación de los datos sin ser detectada; indique claramente al emisor y al destinatario cualquier modificación de los datos; indique con un sello cualificado de tiempo electrónico la fecha y hora de envío, recepción y eventual modificación de los datos.

2. Pruebas electrónicas sin presunción de veracidad

A. Documentos privados consistentes en impresiones o capturas de pantalla:

Por un lado, con documento electrónico privado nos referimos a toda aquella información (textos, hojas de cálculo, imágenes, sonidos, vídeos, bases de datos,

[98] El PDF incorporará un Código Seguro de Certificación (CSV) para asegurar la trazabilidad del original con la copia que se imprima, ya que mediante este código se puede consultar el original electrónico en cualquier momento a través de Internet, accediendo a su enlace con plena validez jurídica.
[99] Es el caso del servicio de BuroSMS o e-SMS que presta el Consejo General de la Abogacía Española. Para más información, hacer clic en el siguiente enlace: https://www.abogacia.es/servicios/abogados/burosms/

facturas[100], etc.) en la que se pueda percibir una manifestación de voluntad o una representación de un hecho de interés para el proceso que requiere de la utilización de alguna TIC para su reproducción[101].

El documento electrónico es cada vez más utilizado, en gran parte, por la normalización de la contratación electrónica. Este sector se encuentra regularizado en los arts. 23 a 28 de la LSSICE. Así, el apartado 1 del art. 24 de esta Ley dispone que "*la prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico […]*". Asimismo, el apartado 2 establece que *"en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental"*[102].

De modo que una de las formas de aportar en un juicio los datos o la información electrónica de las distintas fuentes de prueba (imágenes, palabras o sonidos) puede ser a través del documento electrónico, esto es, en soporte de almacenamiento electrónico (USB, CD o DVD…) según un formato determinado (PDF, Word, JPG, etc.) y susceptible de identificación y tratamiento diferenciado[103].

Por otro lado, cuando hablamos de «pantallazo» hacemos referencia a la captura o congelación de la imagen que se proyecta en un determinado momento en la pantalla

---

[100] En el art. 812 LEC se contienen los casos en los que procede iniciar el juicio monitorio. Este artículo, en su apartado 1.1ª, hace referencia, entre otros, a la factura electrónica cuando prevé como documentos acreditativos de la deuda *"cualquiera que sea su forma y clase o el soporte físico en que se encuentren, que aparezcan firmados por el deudor o con su sello, impronta o marca o con cualquier otra señal, física o electrónica"*.

[101] ILLÁN FERNÁNDEZ, J. M., *op. cit*, pp. 467 y ss. Obra citada por BUENO DE MATA, F., *op cit*., p. 38.

[102] Tal es el caso del Auto de la AP de Barcelona, de 15 de enero de 2018 (Roj: AAP B 15/2018), que en la reclamación de una deuda que deriva de un préstamo bancario contratado vía telemática, estima el recurso de apelación interpuesto por ING BANK y ordena al Juzgado de 1ª Instancia a que admita a trámite el procedimiento de juicio monitorio, al considerar que el motivo del juzgado de instancia, por el que se rechaza la demanda, no puede aceptarse, ya que de los documentos que aporta la solicitante se infiere, "como mínimo indiciariamente", que no son obstáculo para admitir a trámite dicho procedimiento porque de ellos puede salir un juicio de suficiencia deducido de la prueba aportada que exige el artículo 815.1 de la Ley de Enjuiciamiento Civil. Además, señala que *"la ley procesal debe ser interpretada en atención a los nuevos avances tecnológicos y cada vez es más frecuente que las empresas tiendan a eliminar el soporte físico de papel, registrando todos los documentos y datos en los archivos informáticos, ya que el volumen de trabajo de cualquier empresa medianamente importante hace inviable el archivo físico del papel".*

[103] DELGADO MARTÍN, J., *op. cit.*, pp. 54 y 55.

de un dispositivo electrónico (*smartphone*, *tablet*, ordenador…), el cual la realiza por sí mismo (también se puede fotografiar a través de la cámara de otro dispositivo).

Estos pantallazos podrán tener acceso al proceso por medio de soporte papel[104], a través de su impresión, o directamente en el mismo soporte electrónico en el que se haya originado. Si bien, el valor probatorio que le dé el Juzgador o Tribunal a tal documento (electrónico u ordinario), dependerá de las posturas procesales que adopten las partes y de la valoración conjunta que falle sobre las pruebas practicadas[105] (como más adelante veremos).

a. Correos electrónicos

El correo electrónico o e-mail (*electronic mail*) era la aplicación de intercambio de datos más utilizada de Internet hasta que las redes sociales y los programas de mensajería instantánea irrumpieron en la sociedad.

Los usuarios de las plataformas de e-mail (Gmail, Hotmail o Outlook, Yahoo…) disponen de una cuenta identificada con una dirección electrónica, *nick*, o nombre de usuario al que acceden mediante la validación de su contraseña, garantizándose con ello la privacidad de los mensajes que se almacenan en sus servidores[106].

La definición legal de e-mail se encuentra en el art. 2, letra h), de 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 (Directiva sobre la privacidad y las comunicaciones electrónicas). Así, se define como *"todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el*

---

[104] Así, lo prevé la SAP de Santa Cruz de Tenerife, de 27 de marzo de 2012 (Roj: SAP TF 512/2012), cuando dice que la «*impresión de pantalla*» *"no es sino la traslación a soporte papel de un documento electrónico que, como tal, puede ser valorado en los términos legalmente señalados. Y es que como ya ha señalado esta Sección con anterioridad (sentencia de 18 de noviembre de 2009) la entidad actora acompañó con la demanda la copia en soporte papel del documento electrónico que tenía a su disposición..., y hay que tener en cuenta que, primero, la Ley 59/2003, de 19 de diciembre, de firma electrónica* [derogada], *y después la Ley 41/2007, de 7 de diciembre, equipararon plenamente a efectos judiciales los documentos en papel y los documentos multimedia, reformando consecuentemente los arts. 267 , 268 , 318 y 326 de la Ley de Enjuiciamiento Civil".*

[105] DELGADO MARTÍN, J., *op. cit.*, pp. 64 y 65.

[106] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 44.

equipo terminal del receptor hasta que éste acceda al mismo". De esta definición podemos extraer las siguientes conclusiones[107]:

- Es un sistema que permite la remisión de un mensaje por parte de un usuario (emisor) de determinada dirección de correo electrónico a otro usuario (remitente) con otra dirección de correo electrónico mediante una red de telecomunicación.
- Funciona con una arquitectura cliente/servidor: un mensaje de email es creado usando un programa de correo cliente, el cual envía el mensaje a un servidor (*Mail Transport Agent* o MTA, por sus iniciales); este servidor lo redirige al del destinatario, utilizándose para ello protocolos estandarizados de redes.
- El correo electrónico está compuesto, por un lado, del contenido del mensaje junto con sus documentos anexos (textos, imágenes, audios, videos…) y, por otro, de los datos de tráfico (fecha, hora, duración, origen, destino), siendo ambas partes muy útiles a efectos probatorios.
- Cuando el remitente envía un email, no se dirige directamente a su remitente, sino que se envía primero a una serie de servidores que se encargan de redirigirlo, dejando en este sellos o huellas digitales, de forma que se puede localizar la dirección IP desde la cual se ha direccionado el mensaje[108].
- Estos mensajes se pueden almacenar durante el tiempo que estimen necesario, tanto el servidor como por el propio cliente, si bien, a pesar de que este último los borre, en ocasiones las operadoras guardan copias de seguridad durante cierto tiempo.

Cuando aportamos un correo electrónico puede surgirnos, entre otros, los siguientes interrogantes procesales: por un lado, la incógnita de la competencia territorial y, por otro, la cuestionabilidad de su autoría y receptación[109]. No obstante, si comparamos una carta manuscrita, presentada por cualquiera de las partes, siempre generará dudas más

[107] DELGADO MARTÍN, J., *op. cit.*, pp. 167 y ss.
[108] FERNÁNDEZ LÁZARO, F.: "Medios técnicos en la investigación de los delitos telemáticos", dentro de la obra, «Los nuevos medios de investigación en el proceso penal. Especial referencia a la videovigilancia», *Cuadernos de Derecho Judicial II*, 2007, Consejo General del Poder Judicial (CGPJ), p. 136. Obra citada por DELGADO MARTÍN, J., *op. cit.*, pp. 168.
[109] BUENO DE MATA, F.: "La interceptación de los e-mails". *Revista Justicia*, 2009, pp. 5 y ss. Obra citada por BUENO DE MATA, F., *op. cit.*, p. 162.

serias acerca de la autoría de su remitente, ya que no conocemos la letra de éste y bien se puede copiar y falsificar su firma (si es la contiene), a diferencia que un carta enviada por correo electrónico, que en la actualidad se puede verificar, de manera relativamente sencilla, al menos la utilización de la cuenta que pertenece al usuario al que se le atribuye la autoría de su contenido, lo que siempre generará más seguridad en este aspecto.

Por lo general, el acceso al proceso de los correos electrónicos será bien a través de la captación de su imagen en un dispositivo electrónico o bien impresos en papel, tratándose por tanto de documentos privados. Sin embargo, se podrán incorporar en un acta notarial para reforzar su eficacia probatoria y evitar así su volatibidad. De esta manera, el documento público que surgiera acreditaría la existencia de tales mensajes, las direcciones de email utilizadas y las fechas en las que se han remitido. Por otro lado, si se impugnen da cualquier manera dichos mensajes, será pertinente aportar un dictamen pericial realizado por un ingeniero informático que aclare la controversia y posibilite que la prueba electrónica despliegue todos los efectos[110] que se deduzcan de ella en el proceso[111].

Asimismo, la acreditación de un correo electrónico puede fundamentarse en la aportación de cualquiera de los dispositivos electrónicos de remisión o recepción del email en cuestión o de la validación de cualquiera de los servidores implicados.

Si bien, cuando los operadores de servicios de telecomunicación se encuentren fuera del territorio de la Unión Europea, será complicado el acceso a los datos que conservan, ya sea en cumplimiento de sus propias políticas de privacidad y protección de datos, o de conformidad a las leyes a las que se deban someter.

---

[110] Un ejemplo del efecto jurídico que puede producir el despacho de un correo electrónico es la interrupción de la prescripción. Así se patentiza por la AP de Baleares en su Sentencia de 8 de noviembre de 2018 (Roj: SAP IB 2071/2018), rechazando el primer motivo de apelación de la parte demandada, esto es, la prescripción de la acción ejercitada, ya que, según dispone este Tribunal: *"partiendo de la fecha que propone la propia parte demandada (31 agosto 2012), por aplicación del artículo 1973 del Código Civil, se habría interrumpido su cómputo a través de la reclamación que la actora giró a la demandada el 2 de julio de 2015 mediante correo electrónico (documento nº6 de la demanda), por lo que, a la fecha de presentación de la solicitud de proceso monitorio (20 septiembre 2016) la acción no habría prescrito"* (FJ Segundo).

[111] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 44.

De esta manera, en España resulta de aplicación la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, a los operadores dichas redes (art. 2). No obstante, el objeto de esta ley se limita a la conservación de los datos de tráfico, localización e identificación de los usuarios registrados -excluyéndose el contenido de las comunicaciones electrónicas- debiéndose ceder tales datos, mediante la oportuna orden judicial[112], únicamente para la investigación, detención y enjuiciamiento de delitos graves (art. 1), por lo que, en principio, no se podrán obtener para el resto de jurisdicciones.

Viene a colación recordar que cuando el acceso a un e-mail se produce antes de que el destinatario lo haya leído, ello afectará de lleno al derecho fundamental del secreto de las comunicaciones, mientras que si se hace cuando ya ha sido leído no, ya que el proceso de comunicación habría finalizado[113], pero podría verse comprometido otro derecho fundamental, esta vez el del art. 18 CE, es decir, la intimidad personal[114].

Finalmente, hay que puntualizar que en los correos electrónicos se puede incorporar una especie de acuse de recibo o «confirmación de lectura» que permite dar la constancia de que el mensaje ha sido recibido y abierto por su destinatario[115] y así evitar la posible impugnación de su recepción. De lo contrario, será fundamental la anuencia a acceder o mostrar el respectivo buzón del correo electrónico de quien niega su remisión para así comprobar si se mostró o no[116].

---

[112] Por el contrario, cuando se trate de datos conservados en cumplimiento de la normativa interna de la operadora, y no estén afectados a procesos de comunicación, podrán ser cedidos a la autoridad policial sin necesidad de recabar autorización judicial, pese a que contengan datos personales y, por lo tanto, se vea comprometido el art. 18.4 CE, ya que el art. 11.2 d) LOPD da la cobertura legal necesaria para ello al habilitar directamente al Ministerio Fiscal.

[113] Tal y como manifiesta el TS en su sentencia de 10 de diciembre de 2015 (Roj: STS 5809/2015), que en su FJ III b) precisa que *"el derecho al secreto de las comunicaciones rige mientras se desarrolla el proceso de comunicación (vid. SSTS 342/2013, de 17 de abril, 786/2015, de 4 de diciembre, ó 859/2014, de 26 de noviembre). Una vez cesado éste, llegado el mensaje al receptor, salimos del ámbito del art. 18.3 CE, sin perjuicio, en su caso, del derecho a la intimidad proclamado en el número 1 del mismo precepto, aunque en este segundo supuesto sin supeditación constitucional imperativa a la autorización judicial".*

[114] DELGADO MARTÍN, J., *op. cit*., pp. 176.

[115] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 44.

[116] DE URBANO CASTRILLO, E., *op. cit.*, p. 51.

b. Aplicaciones y plataformas de mensajería instantánea

Hoy en día prácticamente todo el mundo hace uso de alguna aplicación o multiplataforma de mensajería instantánea, ya sea WhatsApp (la más relevante por ser la más utilizada), Telegram, Skype, Messenger (Facebook), etc. Sus principales características son:

- Permiten el intercambio de conversaciones entre sus usuarios bien a través de sus aplicaciones (*softwares*) para smartphones, tablets, smartwatches u ordenadores, bien por medio del acceso a sus plataformas online, por las cuales se pueden realizar llamadas y videollamadas (bilaterales o grupales), además de compartir toda serie de contenidos, desde mensajes de texto, a música, grabaciones de voz, fotos, gifs[117], *stickers* (pegatinas), ubicaciones, historias, videos o contactos.
- A diferencia de los SMS, estás plataformas funcionan utilizando Internet. Asimismo, en virtud del llamado «cifrado de extremo a extremo» (*end-to-end*) se garantiza la confidencialidad de las comunicaciones[118] y, por tanto, los datos intercambiados no se mantienen en un servidor externo[119], es decir, solo pueden acceder a ellos sus interlocutores (ni siquiera puede la propia compañía), ya que los mensajes se cifran con un candado y código (llave) único que solo poseen el emisor y el receptor y, por tanto, los datos son almacenados únicamente por sus usuarios, bien internamente en sus respectivas cuentas o; bien externamente mediante copias de seguridad en la memoria de sus dispositivos electrónicos o en la nube (Google Drive, Drive, OneDrive, iCloud…). Ello implica que, aunque se intervengan judicialmente todas las comunicaciones desde el terminal de una persona investigada por las

[117] Sus siglas provienen de la expresión inglesa 'Graphics Interchange Format', lo que viene a ser en español, Formato de Intercambio de Gráficos. Se trata de un archivo gráfico (imágenes fijas u animadas) cuya extensión es .gif. Para más información visítese el siguiente enlace: https://definicion.de/gif/

[118] *Vid.* "WhatsApp: qué es el cifrado «end to end» y por qué es importante". *ABC*. Disponible en: https://www.abc.es/tecnologia/consultorio/abci-whatsapp-whatsapp-cifrado-201604060948_noticia.html?ref=https:%2F%2Fwww.google.com%2F

[119] No es el caso de Skype o Messenger (a las que se puede acceder utilizando un navegador de internet a través de sus respectivas páginas web), ya que estas guardan (la primera de forma temporal y la segunda permanentemente) las conversaciones para que podamos tener acceso a las mismas en diferentes dispositivos. Para más información véase el siguiente enlace: https://miracomosehace.com/donde-guarda-almacena-skype-fotos-archivos-conversaciones-grabaciones/

Fuerzas de Seguridad del Estado, los mensajes de WhatsApp aparecerán encriptados en la plataforma SITEL (Sistema Integrado de Interceptación Telefónica) y, por lo tanto, no serán legibles[120].

Como todo sistema informático, existe la posibilidad de ser alterados remotamente (o si se tiene acceso al mismo, directamente). También se pueden suplantar las cuentas de sus usuarios, por ello, la aludida STS 300/2015 (Sala 2ª), de 19 de mayo, invoca la llamada cautela al considerar que *"la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido".* Asimismo, la STS 5421/2015, de 27 de noviembre, reiterando esta doctrina, dispone que, *"únicamente con un informe pericial que identifique el teléfono emisor de los mensajes delictivos, a salvo de cumplido reconocimiento, o prueba testifical que acredite su remisión, pueden dar cobertura probatoria a la autenticidad del mensaje en cuestión. En efecto, 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 superchería".*

Es cierto que los riesgos de manipulación son altos, por ejemplo, la aplicación de WhatsApp permite eliminar mensajes en un tiempo máximo de una hora de haberlos enviado[121], haciendo desaparecer con ello las posibilidades de adquirir la constancia del

[120] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 71

[121] Tal y como se informa en la página web oficial de WhatsApp en el siguiente enlace: https://faq.whatsapp.com/android/chats/how-to-delete-messages/?lang=es

contenido de esos mensajes para terceros. No obstante, existen MODs (o versiones) no oficiales de esta aplicación que permiten, entre otras cosas, que estos mensajes borrados sigan reflejándose en la pantalla del dispositivo que tiene instalada dicha versión "pirata" de WhatsApp[122].

Sin duda, la incorporación al proceso del contenido de un mensaje o conversación mantenida en una aplicación o plataforma de mensajería instantánea puede producirse a través de un medio probatorio o cumulativamente mediante varios: se puede hacer entrega y custodia del smartphone en el que se encuentre la conversación o se autorizar el acceso a la plataforma en cuestión dando el nombre de usuario y su clave para que se produzca el reconocimiento de su contenido por parte del juzgador; también se podrá solicitar el cotejo del LAJ para que proceda a la transcripción de los textos y a la descripción de los archivos que se contengan en dichas redes de mensajería; asimismo, se podrá interesar un examen pericial (que recaerá sobre el dispositivo electrónico) o la declaración testifical o el interrogatorio de parte acerca del contenido de la documental proveniente de los pantallazos tales aplicaciones[123] e incluso, como hemos dicho, podríamos interesar varios de ellos para darles una fuerza probatoria adicional y evitar así que prospere la más que probable impugnación de la parte contraria.

Desde luego, lo recomendable es presentar físicamente el dispositivo electrónico (que normalmente será un smartphone) al proceso judicial junto con una copia escrita o «pantallazo» impreso para que sean cotejados los mensajes relevantes para la controversia o incluso en el propio acto del juicio o vista se podrán reconocer y examinar directamente por el órgano judicial (arts. 353 y ss LEC). De igual forma se podrá aportar un acta notarial que de fe y transcriba el contenido de tal conversación objeto de prueba.

En estos casos, la prueba será totalmente válida y estimada conforme a la sana crítica de no haber oposición por ninguna de las partes. De lo contrario, dicha prueba será valorada conjuntamente con los restantes medios probatorios, los motivos de

---

[122] Es el caso del conocido MODs llamado GBWhatsApp que, junto con WhatsApp Plus, es el más utilizado, tanto es así que existen varias versiones como la DELTA. Más información en: https://www.malavida.com/es/soft/gbwhatsapp-delta/android/#gref

[123] ALONSO-CUEVILLAS, J.: "Internet y prueba civil", *Revista Jurídica de Catalunya*, nº4, 2001, p. 1078. Obra citada por DELGADO MARTÍN, J., *op. cit*., p. 181.

impugnación (elementos de corroboración de la existencia y contenido de los mensajes que se pretenden probar) y las manifestaciones vertida por los intervinientes (partes procesales, testigos y peritos). Por ejemplo, en el caso de conversaciones de grupos de Whatsapp o Messenger (supuestos de comunicación multidireccional), igualmente podremos aportar otro dispositivo electrónico de uno de los miembros del grupo, que habrá de ser citado a efectos de que ratifique la realidad de dichos mensajes[124].

Por otro lado, es importante poner de relieve el sistema de verificación de WhatsApp, el cual te identifica a través de la introducción de número de teléfono del titular que va a acceder a la aplicación, comprobándose esto mediante un código que es comunicado a ese número para que se confirmen tales datos. De esta manera, es más fácil averiguar quién envía los mensajes, o al menos desde qué número, ya que este estará atribuido a alguien que ha contratado una línea telefónica y, para ello, la Ley 25/2007, de 18 de octubre (de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones) obliga a identificar debidamente, mediante la puesta a disposición de sus datos personales, a la persona contratante (usuario telefónico). Por ello, si fuera negado la autoría o envío de los mensajes objeto de debate, sería razonable que se invirtiera la carga de la prueba a la misma y le correspondiera acreditar las circunstancias que lo avalen[125], tales como el acceso ordinario a su teléfono móvil por terceros o la sustracción o pérdida del dispositivo (mediante la oportuna denuncia previa).

En definitiva, los supuestos en los que los Juzgados o Tribunales admiten como prueba documental una conversación o mensaje de aplicaciones de mensajería instantánea son los siguientes: A) cuando la parte interlocutora de la conversación no impugna la

---

[124] DELGADO MARTÍN, J., *op. cit*., p. 183.

[125] Así lo concluye la AP de Pontevedra en su sentencia de 31 de mayo de 2017 (Roj: SAP PO 1081/2017) en la que la parte demandada recurre la primera instancia invocando error en la valoración de la prueba al no haber quedado acreditada por la parte demandante la "autenticidad" de las comunicaciones, mensajes, whatsapps, aportados con la demanda y, por tanto, haberse producido una inversión de la carga probatoria, mencionando a tal efecto la jurisprudencia del TS (comentada anteriormente) y la facilidad de manipulación y la supuesta inseguridad de WhatsApp, lo que desestima la Audiencia argumentando que tal jurisprudencia es de la Sala de lo Penal (donde impera la presunción de inocencia) y, por ello, es necesario identificar el origen de la comunicación, sus interlocutores y destacar la integridad de su contenido por quien aportar y se apoya en dicha prueba, siendo conveniente para ello (no indispensable) completar con el dictamen de un experto informático. En cambio, dice la sentencia, que en la jurisdicción civil *"nada impide, con las debidas cautelas, el valorar la validez y alcance de tales mensajes una vez alcanzada la certeza sobre su origen, identidad de los interlocutores y contenido"* (en alusión al principio de libre valoración por parte del juzgador que tienen este tipo de pruebas).

conversación; B) cuando reconoce expresamente dicha conversación y su contenido; C) cuando se comprueba su realidad mediante el cotejo con el otro terminal implicado (exhibición); D) cuando se practica prueba pericial que acredita la autenticidad y envío de la conversación[126].

c. Páginas web y redes sociales

No cabe duda de que la información que se «cuelga» libremente en las redes sociales, blogs, foros, buscadores (en síntesis, páginas web) -como pueden ser comentarios, fotografías, vídeos, historias, directos y demás contenido-, puede llegar a ser muy relevante en cualquier tipo de proceso judicial, siendo la misma mayormente de carácter público, por lo que el acceso a la misma no vulnerará, en la mayoría de casos, ningún derecho fundamental, en concreto nos referimos al derecho a la intimidad o secreto de las comunicaciones[127].

Por un lado, según AGUSTINO y MONCLÚS[128], red social es aquella plataforma tecnológica que permite a sus usuarios, a través de sus perfiles (públicos o semipúblicos), vincularse entre sí, creando de esta manera sistemas cruzados e interactivos de generación y difusión de información.

Por otro lado, podemos definir página web, tal y como señala ABEL LLUCH[129], como una modalidad de documento informático al que se accede navegando por Internet, previa identificación de un enlace. Para interpretar una página web se precisa la instalación de un navegador en el correspondiente dispositivo electrónico inteligente, tales como, Internet Explorer, Chrome, Mozilla Firefox, etc., interpretando todos estos navegadores el lenguaje o código HTML (*Hyper Text Markup Lenguage*, esto es en

[126] ROJAS ROSCO, R.: "La prueba digital en el ámbito laboral ¿son válidos los "pantallazos"? en *La prueba electrónica…op. cit.*, p. 96.
[127] DELGADO MARTÍN, J., *op. cit.*, p. 198.
[128] AGUSTINOY GUILAYN, A. y MONCLÚS, J.: Aspectos legales de las redes sociales. Bosch, 2016, p. 20. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 190.
[129] ABEL LLUCH, X.: "Prueba electrónica", dentro de la obra *La prueba electrónica*, editado por el Instituto de Probática y Derecho Probatorio ESADE y JM Bosch Editor, Barcelona, 2011, p. 201. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 199.

castellano, Lenguaje de Marcas de Hipertexto[130]) en cual están desarrolladas las páginas web.

La probática relacionada con las redes sociales o páginas web se proyecta desde dos perspectivas[131]: 1) cuando nos encontramos con hechos relevantes acaecidos directamente en dichas redes o páginas; 2) cuando la información obtenida en las redes sociales o páginas web puede aportar indicios relevantes por estar relacionada con otros hechos objeto de pleito no acaecidos en aquellas.

Aquí, el problema que se da es cuando el contenido de una página web o red social es alterado previamente a su aportación al proceso[132]. De esta forma, la información debe ser recogida con rapidez y almacenada para su posterior análisis[133]. Además, es conveniente que se asegure o preserve previamente por un perito informático el *hash* de tal prueba electrónica, o también se puede acudir a los llamados Terceros de Confianza o Prestadores de Servicios de Confianza Digital (*Trusted Third Party*, TTP) para que certifiquen la autenticidad de sitios web[134] o almacenen registros de los cambios que han sufrido éstos, pudiendo además consultar el contenido de tales páginas en una fecha concreta[135]. Es el caso de la conocida *Wayback Machine* (archive.org)[136]. Incluso la

---

[130] Para más información sobre qué es HTML, véase la siguiente página escrita por Javier Flores Herrera: https://codigofacilito.com/articulos/que-es-html

[131] DELGADO MARTÍN, J., *op. cit*., p. 193.

[132] PICÓ I JUNOY, J.: "Preguntas con respuesta. La prueba a consulta II. Reconocimiento judicial y nuevas tecnologías ¿pueden las partes proponer el reconocimiento judicial para que el Juez perciba el contenido de una página web o de e-mail?", *Cuadernos de Probática y Derecho Probatorio, nº5, Diario LA LEY*, nº7677, 2011, p. 29. Obra citara por ARRABAL PLATERO, P., *op. cit*., p. 310.

[133] UNODC (*United Nations Office on Drugs and Crime*), *Comprehesive Study on Cybercrime*, United Nations, New York, 2013, p. 122. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 194.

[134] El art. 3.17 Reglamento e-IDAS define el «certificado de autenticación de sitio web», como *"una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado"*.

[135] Así lo recomienda Luis Enrique García, responsable de Garón Abogados, en un caso de desahucio por subarriendo por parte de una inquilina, la cual publicitaba el piso arrendado en la conocida plataforma de alquileres turísticos Airbnb, demostrándose tales hechos, entre otras formas, obviamente con la aportación de los respectivos anuncios. Por ello, este abogado explica manifiesta que "cuando se tengan indicios suficientes de que el inmueble objeto de contrato se encuentra en una plataforma de alquileres turísticos se acuda a certificar la página web con el inmueble en cuestión, bien por vía notarial o por cualquiera de las plataformas virtuales conocidas como terceros de confianza. Acto seguido, requerir el cese inmediato y desaparición de la publicación bajo apercibimiento de resolución de contrato", concluye. Disponible en: https://www.expansion.com/juridico/sentencias/2020/12/31/5fdc8967e5fdead32e8b4659.html

[136] ARRABAL PLATERO, P., *op. cit*., p. 310.

página web de la Guardia Civil[137] en colaboración con la empresa "eGarante", ha implementado dentro de su portal de colaboración ciudadana ("COLABORA") la posibilidad de certificar los contenidos de una página web de la que se quiera informar por contener algún hecho ilícito.

Finalmente, queremos hacer alusión a la cuestión que se suele generar acerca de la autoría que se genera en un determinado perfil social y que se atribuye a una persona concreta. Pues bien, simplemente exponer que en la práctica judicial se tiende a presumir que el titular de un perfil o sitio web es el autor de la información que en algún momento ha colgado en ellos, de no rechazarse por el mismo tal hipótesis. Por el contrario, si a quien se le achaca su divulgación lo rebate, el Juez o Tribunal analizará las razones de impugnación alegadas -como puede ser bien que le han hackeado o robado la cuenta o página, o bien que otra u otras personas conocen su contraseña de acceso a su cuenta y le han gastado una broma-, otorgando mayor o menor credibilidad a dicha autoría[138] (por ejemplo, si se acredita con una denuncia previa lo alegado).

d. SMS y MMS

El SMS (*Short Message Service*) es un servicio para titulares de teléfonos móviles que permite enviar exclusivamente mensajes de texto entre estos dispositivos de 160 caracteres[139], a diferencia de los MMS (*Multimedia Messaging Service*), en los que se puede adjuntar pequeños archivos de sonido, video e imagen. Ambos constituyen una aplicación imprescindible de cualquier teléfono móvil. Su sistema de funcionamiento puede sintetizarse alrededor de los siguientes factores[140]:

[137] Para más información abrase el siguiente enlace: https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1236
[138] DELGADO MARTÍN, J., *op. cit.*, p. 196.
[139] Dicha cantidad se ha corroborado, efectivamente, con la aplicación de SMS de un smartphone.
[140] DELGADO MARTÍN, J., *op. cit.*, pp. 167 y ss.

- Cuando un usuario contrata una línea de telefonía móvil, se ha de identificar[141] debidamente para que se le haga entrega de una tarjeta SIM[142] (*Suscriber Identity Module*), para utilizarse en cualquier terminal o dispositivo electrónico de telefonía. Asimismo, a estos últimos se les vincula un número de identificación o IMEI (*International Mobile System Equipment Identity*).
- Cada SMS o MMS es emitido por un determinado teléfono móvil (identificado con el número IMEI) que utiliza una concreta línea telefónica (identificada con una tarjeta SIM) y este llega a su servidor telefónico o SMSC (por sus siglas en inglés, *Short Message Service Center*), el cual lo reenvía automáticamente al número de teléfono de su destinatario (con su propio IMEI, SIM y línea telefónica).
- Se trata de un sistema de almacenamiento y envío. Ello permite acceder a los mensajes que se envían a través de cualesquiera dispositivos móviles, ya que el contenido de los mensajes se aloja en dichos servidores hasta que son entregados a sus destinatarios[143]. En cambio, los mensajes de WhatsApp, únicamente se alojan en los teléfonos de sus usuarios[144].

Los SMS conforman una prueba electrónica fundamental en muchos casos. Ejemplo de ello es la SAP de Cuenca de 30 de junio de 2009 (Roj: SAP CU 301/2009) en la que en su FJ I se está de acuerdo con la presunción de paternidad que establece el juzgador de instancia, gracias en gran parte a que la demandante (amante) presentó unos SMS que correspondían con el número de teléfono de la empresa del demandado (casado), y que fueron transcritos en presencia de las partes y sus letrados, bajo la fe del

---

[141] En cumplimiento de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que en su DA única establece la obligación de los operadores de servicios de telefonía móvil de llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente prepago, ya que antes de la entrada en vigor de esta ley existía un cierto descontrol que daba lugar a que se produjeran, con impunidad, toda una serie de operaciones ilícitas.

[142] Anteriormente, todas las tarjetas SIM venían necesariamente con un PIN (*Personal Identification Number*), sin embargo, hoy en día, al tener ya los smartphones la posibilidad de establecerles contraseñas o sistemas de bloqueo, muchas de estas tarjetas prescinden del número PIN y, por ende, del número PUK (*Personal Unlocking Key*). Este se utiliza cuando se bloquea la tarjeta al introducir erróneamente varías veces el PIN (alrededor de cuatro oportunidades).

[143] Si bien, dichas conversaciones están amparadas bajo el secreto de las comunicaciones que prevé el art. 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en concordancia con los artículos 18.3 y 55.2 de la Constitución

[144] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 45.

LAJ. De esta manera hizo valer los mismos como prueba inequívoca de "la existencia de una relación sentimental y con contenido sexual entre la persona que los enviaba y quien los recibió". También se pronuncia el Tribunal acerca de la cuestionable autenticidad de los SMS y de su posible manipulación. Si bien de manera intranscendente, ya que da más importancia a que el demandado reconoce que los mensajes proceden del teléfono de su empresa (que, según él, estaba al alcance de más personas) y a su negativa injustificada de someterse a las pruebas biológicas que le fueron requeridas[145].

La plenitud probatoria de las comunicaciones realizadas a través de SMS se centra en tres elementos: el remitente del mensaje y su dispositivo telefónico; el destinatario que lo recibe a través de su terminal; y la mismisidad del contenido del mensaje[146].

El destinatario suele ser la persona que aporta al proceso el contenido del mensaje, por diferentes medios probatorios que son valorados por el juzgador o tribunal de conformidad con las reglas de la sana crítica, sin que suponga un problema cerciorarse acerca de que quien lo presenta sea su verdadero destinatario.

En cambio, resulta complicado precisar la identidad del remitente. Por ello, de ser necesario, se tendrá que requerir a la autoridad judicial a que lleve a cabo las actuaciones necesarias para comprobar la identidad del titular del número del teléfono móvil (asociado a una tarjeta SIM, que a su vez lo estará a los datos de su dueño), y una vez se constate la personalidad del titular, citarle para que comparezca y diga si ha sido el mismo el que ha confeccionado dicho mensaje objeto de controversia o pleito o, por el contrario, ha podido tener acceso a su dispositivo un tercero. Asimismo, podrá alegar la falta de autenticidad y de entereza del contenido de los SMS, algo que sin duda puede ocurrir en la realidad dada la cantidad de aplicaciones que permiten la elaboración *ex novo* de mensajes

[145] De modo muy similar se pronuncia la AP de Pontevedra en su Sentencia de 13 de junio de 2018 (Roj: SAP PO 1302/2018). En esta ocasión, dada su actualidad, se presentan mensajes de Whatsapp (cotejados por el LAJ), por lo que el Tribunal refrenda la versión mantenida por la demandante y estima su acción de reclamación de filiación no matrimonial.
[146] DELGADO MARTÍN, J., *op. cit.*, pp. 178 y 179.

simulados o editar su contenido o incluso sus metadatos (hora, fecha, remitente, destinatario…)[147].

Para evitar la problemática anterior, siempre se podrá acudir a un prestador de Servicios de Confianza para que quede constatado el contenido y momento exacto de las comunicaciones que se lleven a cabo, esto es, a través del envío de SMS certificados o BuroSMS (e-Mensajes).

B. Documental consistente en la reproducción y transcripción de archivos multimedia

Los arts. 382 a 384 LEC regulan la aportación de los archivos electrónicos. Así, el primero de ellos, en su primer apartado, prevé como forma de presentación cualquier soporte que sea idóneo, siendo la lista que aparece meramente ejemplificativa y terminando con una cláusula que hace la misma flexible a otros medios nuevos que pudieran darse (*numerus apertus*). Si bien, el segundo inciso indica perceptivamente que, al proponer esta prueba, se acompañará (en su caso) transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el asunto. Por lo tanto, si no se presenta dicha prueba junto con su correspondiente transcripción, el juzgado o tribunal requerirá su aportación bajo apercibimiento de inadmisión en caso de omisión de la petición judicial[148].

a. Grabaciones de audio

Para que una grabación de sonido pueda producir efectos probatorios, el magistrado ABEL LLUCH[149] indica que deberán observarse una serie de garantías, tales como el respeto a la intimidad, la puesta a disposición al Juzgado o Tribunal de los soportes que registran la conversación y la verificación de la autenticidad para evitar posibles manipulaciones.

[147] PÉREZ ASTUDILLO, N. E.: "Los medios telemáticos como prueba de cargo en el proceso", *Cuadernos Digitales de Formación*, nº 3, 2015, p. 6. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 179.
[148] VERGÉS CORTIT, R.: "Instrumentos de Archivos de Datos", en *La prueba civil a debate judicial. Estudios prácticos sobre prueba civil I* (VVAA). Wolters Kluwer, Madrid, 2018, pp. 211 y 212.
[149] ABEL LLUCH, X., *op. cit.*, pp. 206 y 207. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 47.

Así, para que no se vea afectado el derecho a la intimidad o al secreto de las comunicaciones, quien presente una grabación de voz deberá haber sido participe o el destinatario de la misma, ya que, de lo contrario, de tratarse de una grabación entre terceros o dirigida a un tercero, se estará vulnerando dichos derechos fundamentales reconocidos en el art. 18 CE[150] (a no ser que su contenido pueda constituir un delito y se haya obtenido su acceso de manera fortuita). Cuestión distinta sería la difusión pública de quien graba una conversación mantenida con un tercero o recibe mensajes de voz[151].

En el caso de que se impugne su autenticidad, debido a la más que probable falta de la misma, el citado Magistrado nos da al respecto dos posibilidades a tomar: A) realizar un «cotejo de voces» para así contrastar el registro fonográfico con el tono y sonido de voz de la persona a la que se le atribuye; B) aportar un dictamen pericial tecnológico que recaiga sobre el soporte que recoge directamente la grabación con el objetivo de verificar que no ha sido modificado o ni ha sufrido alguna alteración.

Por lo que concierne a la primera posibilidad, MONTÓN REDONDO[152] nos da las pautas a seguir durante el proceso de «cotejo de voces»:

- Se reconstruye un "cuerpo de voz" delante del órgano judicial, las partes y el LAJ.
- En ella se repetirán varias veces la oración grabada y cuestionada.
- Después, se grabará dicho "cuerpo de voz" en un dispositivo igual o similar al que recogió la grabación original.
- En estos casos, puede resultar de gran ayuda la comparecencia de testigos que conozcan la forma de hablar de la persona para que manifiesten si corresponde o no.

[150] STC 114/1984, de 29 de noviembre (BOE núm. 305, de 21 de diciembre de 1984).
[151] Podría constituir una intromisión ilegítima a la intimidad, honor o propia imagen (art. 7 LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen), o incluso un delito de revelación de secretos del art. 197 CP.
[152] MONTÓN REDONDO, A.: "Medios de reproducción de la imagen y el sonido", *Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial (CGPJ), nº7,2000, p. 190. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., pp. 47 y 48.

- Una vez terminado, deberá estudiarse la grabación técnicamente, mediante una escucha crítica, estudio frecuencial, espectográfico y ambiental para determinar la correspondencia entre las voces.

b. Vídeo-grabaciones

La grabación de imágenes digitales en vídeo es otro medio de prueba electrónica que puede aportarse a un proceso judicial.

Recientemente, el TC, en su sentencia de 19 de noviembre de 2020[153], ha declarado inconstitucional el inciso "no autorizado" del art. 36.23 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC) -y, por conexión, del art. 19.2 de la misma ley-, al prever como infracción grave el uso no autorizado de imágenes o datos personales o profesionales de las autoridades o miembros de las Fuerzas y Cuerpos de Seguridad, por chocar con el art. 20.2 CE, ya que se condiciona ello a la obtención de autorización administrativa previa y, asimismo, el derecho de información amparado por el art. 20.1 d) CE, se ve afectado por una restricción previa y desproporcionada, al establecerse una censura previa -lesiva del art. 20.2 CE- y además permitirse el secuestro no judicial de material informativo, en contradicción con el art. 20.5 CE. Entre otras cuestiones, esto conlleva implícitamente que un ciudadano pueda grabar con total libertad la actuación de un agente de la autoridad cuando éste le impone una denuncia, para de esta forma poder quebrar la presunción de veracidad de la que gozan los funcionarios y, así, no verse el particular completamente indefenso, es decir, en igualdad de armas.

Podemos añadir un caso controvertido de videograbaciones realizadas por aeronaves no tripuladas, más conocidas como drones[154]. Pues bien, la pregunta que nos

[153] Sentencia del Pleno del Tribunal Constitucional 172/2020, de 19 de noviembre de 2020

[154] Igualmente, encontramos el Modo Centinela de los vehículos Tesla, semejante al de las cámaras *on board* instaladas en otros vehículos. Se trata de una alarma avanzada que emplea las cámaras del 'Autopilot' programa que se activa cuando detecta posibles amenazas contra el vehículo, como la aproximación de alguien hacia el mismo, mostrando un mensaje en su pantalla táctil advirtiendo que el sujeto que se acerca está siendo grabado por las cámaras que dispone el vehículo alrededor y dentro de sus compartimentos. Para más información visítese el siguiente link: https://www.autofacil.es/legal/2019/05/23/camara-on-board-denunciar-conductor/50382.html

hacemos es qué pasaría si recogemos con uno de estos aparatos hechos que podrían utilizarse como prueba en un procedimiento judicial.

En caso de que así fuera, estaríamos ante una confrontación de derechos fundamentales, entre el derecho a la prueba del art. 24 CE y el art. 7 de la Ley Orgánica, de 5 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[155], la cual habría de ser valorada por el juzgador[156].

Otro caso controvertido es el de cámaras *on board*, muy utilizadas por conductores de países como Rusia o China, en los cuales, ante la afluencia de viandantes que se lanzaban a los coches para intentar con ello cobrar una indemnización -ya que la ley de dichos países les ampara con presunciones objetivas de culpabilidad sobre el conductor- se han visto prácticamente obligados a llevar dichos dispositivos instalados.

Mario Arnaldo[157], presidente de Automovilistas Europeos Asociados, declara que grabar con este tipo de cámaras mientras se conduce es completamente legal, *"siempre y cuando, con la reproducción del vídeo, no se atente contra el derecho a la intimidad de las personas* [por ejemplo, no se puede grabar el interior de una vivienda; un vehículo no cuenta con la misma categoría de protección a la intimidad que una vivienda, aunque se trate también de una propiedad privada] *o contra el derecho a la propia imagen"* -no se puede divulgar la imagen de una persona sin su consentimiento-.

---

[155] DE PRADA RODRÍGUEZ, M.*: op. cit*., p. 342.

[156] No está de más traer a colación una de las conclusiones que obtuvo la Autoridad Catalana de Protección de Datos en su Informe publicado en 2014, que tiene su origen en una consulta planteada por una universidad sobre el ejercicio de los derechos ARQUEO en el uso de "drones", y es que *«la utilización de drones que conlleve la captación de imágenes de personas físicas identificadas o identificables se regirá por los principios y obligaciones de la LOPD. Las particularidades de este tratamiento de datos no eximen, en principio, al responsable de cumplir con el deber de información a los afectados (art. 5 LOPD). […]. En el caso de uso de drones en espacios abiertos delimitados, la información también podría facilitarse mediante la colocación de estos carteles informativos. En caso de espacios abiertos no delimitados, el responsable podría plantear ante esta Autoridad, a la vista de las circunstancias concretas concurrentes en cada caso, si las medidas que pretende adoptar para facilitar a los interesados la información relativa al ejercicio de los derechos ARQUEO se adecuan a la normativa de protección de datos»*. URL: https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercador/cercador-detall/CNS-12-2014-00001.

[157] ESPINÓS, ENRIQUE: "¿Puedo usar una cámara on board para denunciar a otro conductor?". *Autofácil*. Disponible en: https://www.autofacil.es/legal/2019/05/23/camara-on-board-denunciar-conductor/50382.html

Por eso, *"y si se presenta una grabación como prueba en un caso de siniestro* [como podría ser para mostrar que la culpa del otro conductor en un golpe], *será el juez el que tenga que valorar siempre la grabación como prueba y declararla procedente o no"*, continúa Arnaldo. *"Para ello, tendrá que tener en cuenta:*

1.- Que se haya obtenido legalmente.

2.- Que su reproducción no vulnere ni el derecho a la intimidad ni a la propia imagen de las personas.

3.- Pero también que la grabación esté justificada o sea pertinente para el esclarecimiento de un delito o falta.

4.- Que se garantice su inalterabilidad; esto es, que no haya podido ser modificada o editada. Si una grabación cumple estos requisitos, un juez debería considerarla válida como prueba", concluye el presidente de la asociación de Automovilistas Europeos.

c. Fotografías digitales

Una cámara digital se compone, al igual que una analógica, de se respectivo objetivo, obturador y diafragma. No obstante, en lugar de proyectar la imagen sobre un negativo, se proyecta sobre un sensor CCD (*Charge Coupled Device*) que transforma la imagen en *bits* (código binario en escala de grises o a color), guardándose las imágenes en una memoria. De esta manera, se pueden transferir a otros dispositivos electrónicos para almacenarlas, copiarlas, reproducirlas o editarlas[158].

La principal ventaja que tiene la fotografía digital sobre la analógica es su perdurabilidad, en contraposición a la mayor facilidad y amplitud para modificar las primeras frente a las segundas.

Alguno de los inconvenientes que suelen surgir en la práctica de esta prueba electrónica son[159]:

[158] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., pp. 50 y 51.
[159] *Ibidem.*

Primeramente, los Letrados frecuentemente impugnan el valor probatorio de las fotografías porque no acreditan con seguridad el momento y el lugar en las que se tomaron, aún contando las mismas con marcas de agua (fecha y hora), ya que bien podría haberse interpuesto la misma a la imagen en beneficio de la parte que la presenta a sabiendas de su falsedad. Una manera de solventar esto es requerir a un Notario que extienda un acta de presencia en un determinado lugar que se documentará con distintas fotos. De modo que, la fuerza probatoria de la fe pública se extenderá como mínimo a que dicho lugar se corresponde con la dirección indicada por el requirente y a que, en la fecha en que se hicieron las fotografías, se encontraba dicho lugar en el estado que se refleja.

Otra posible solución que nos da los autores de la obra *La prueba en la era digital*, es hacer uso de la aplicación para *smartphones* llamada 'Acta mobile'[160]. Como se describe en su página web, se trata de un servicio de captura de imagen y posición GPS para smartphones en un entorno seguro (SSL 256) con garantía de integridad, acceso securizado y fechado de tiempo (*TimeStamping*), con la intermediación de 'ColorIURIS' (Prestador de Servicios de Confianza), el cual garantiza la integridad de la captura en fecha y hora ciertas, con plenos efectos de prueba ante los Tribunales, custodiando una copia de la captura junto al resumen hash del original durante cinco años.

Finalmente, los Letrados acostumbran impugnar el valor probatorio de las imágenes digitales alegando la gran facilidad que tienen éstas de ser manipuladas. Por ello, para evitar estas situaciones, lo conveniente será aportar un dictamen pericial informático que verifique que los archivos fotográficos no han sufrido alteraciones y se corresponden con los originales, tomados en su momento.

[160] Para saber más véase el siguiente link: https://www.coloriuris.net/acta-mobile/info/saber-mas/

VI. APORTACIÓN Y ADMISIBILIDAD DE LA PRUEBA ELECTRÓNICA

Ante todo, es menester en el proceso civil para la aportación de una prueba en el mismo, que primero se pida su admisión, y para ello se habrán de cumplir una serie de reglas que vamos a detallar en los próximos epígrafes.

Asimismo, el momento de acompañamiento y petición de la prueba está sujeto al principio de preclusión del art. 271 LEC, que se designa como "Preclusión definitiva de la presentación y excepciones a la regla". Según este artículo, no se admitirá ninguna evidencia que se presente después de la vista o juicio (salvo las excepciones que se prevén en el apartado 2). Mismamente, el art. 269 del mismo texto legal, prevé como consecuencias de la falta de presentación, designación o anuncio de la prueba junto con la demanda o contestación (o en su caso en la audiencia previa) la pérdida de la oportunidad de presentarla o solicitarla posteriormente, salvo que se trate de hechos posteriores o desconocidos y no imputables a la parte que los alega (art. 270 LEC).

Finalmente, la Sentencia de 20 de septiembre de 2018 de la AP de Madrid[161], en sede penal, señala que, en el mundo digital, las formas en las que las fuentes de prueba acceden al proceso puede realizarse a través de la utilización de cualquiera de los medios de prueba previstos legalmente, esto es, como prueba documental, pericial, testifical, o de interrogatorio de parte (FJ Tercero). En todo caso, consideramos que en el proceso civil habrá de tenerse en cuenta lo dispuesto en el art. 384 LEC[162], es decir, que podrán aportarse como prueba documental, tanto en soporte papel (tradicional), como en los

[161] Sentencia de la Audiencia Provincial de Madrid (Sección 27) de 20 de septiembre de 2018 (Roj: SAP M 15080/2018).

[162] Así, este artículo establece: *"1. Los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que, por ser relevantes para el proceso, hayan sido admitidos como prueba, serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar y de modo que las demás partes del proceso puedan, con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga.*
2. Será de aplicación a los instrumentos previstos en el apartado anterior lo dispuesto en el apartado 2 del artículo 382. La documentación en autos se hará del modo más apropiado a la naturaleza del instrumento, bajo la fe del Letrado de la Administración de Justicia, que, en su caso, adoptará también las medidas de custodia que resulten necesarias.
3. El tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza".

diferentes soportes informáticos "que permitan archivar, conocer o reproducir datos relevantes para el proceso".

1. Límites en la obtención de las pruebas electrónicas

Por un lado, si el documento electrónico no pertenece, o no fue creado por la persona que lo aporta, será ilícita su obtención y aportación por persona no autoriza, al violentarse de esta manera el derecho fundamental a la intimidad personal (art. 18 CE) y, por tanto, deberá ser inadmitido por el juez, además de omitir éste su contenido por completo, en aras a tomar una decisión final acerca del asunto que se debate.

Por otro lado, si la prueba que buscamos no está en nuestro poder y tampoco nos la facilitan, hemos de requerir al juzgado que la solicite o investigue acerca de su paradero, para que, una vez localizada y obtenida, su *iter* probatorio sea legal.

Sin embargo, esto último no siempre se podrá llevar a cabo, ya que en el proceso civil se limita la obtención a que en este itinerario no se vea comprometido ninguna clase de derecho fundamental previsto en la CE.

Así, como ejemplos, podemos poner los documentos que estén sometidos a secreto profesional (arts. 20 y 24 CE). Este derecho está desarrollado, entre otras, en la Ley 1/2019 de 20 de febrero, de Secretos Empresariales[163], en la Ley 7/2006, de 31 de mayo, del ejercicio de profesiones tituladas y de los colegios profesionales[164], y como no, el Estatuto General de la Abogacía. Al amparo de estas disposiciones, y otras concordantes, los archivos digitales que traigan su causa como consecuencia de una actividad profesional estarán protegidos bajo secreto profesional y, en teoría, no podrían hacerse valer en un juicio.

---

[163] De esta manera su art. 1 lo define como *"cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto".*

[164] Esta Ley establece en su art. 10 que *"los profesionales titulados tienen el deber del secreto profesional, de acuerdo con la Constitución española y la legislación específica de aplicación".*

Nótese que se dice "en teoría", porque existen numerosos supuestos en los que, por ejemplo, se aportan en procesos contenciosos conversaciones mantenidas por email entre letrados contrarios, y a pesar de ser estas impugnadas por estar sometidas a secreto profesional, Su Señoría las admite como pruebas válidas al considerar que prevalece sobre este deber el derecho fundamental a la prueba, si bien, con apercibimiento de las consecuencias sancionables que, por parte de su Colegio de Abogados, pueda tener[165].

2. Requisitos de la prueba electrónica en la aportación para su admisión

Toda prueba, sea electrónica o no, deberá cumplir una serie de requisitos para que pueda aspirar a ser incluida en un proceso judicial: pertinencia, idoneidad y legalidad.

A ello, debemos añadir que se haya formulado en momento procesal oportuno, que sea relevante para el caso, así como "*que reúna las condiciones de idoneidad objetiva para la acreditación de los hechos que sean relevantes*" (STC 236/2002, de 9 de diciembre).

A sensu contrario, no serán admisibles las pruebas que busquen únicamente dilatar del proceso, las antieconómicas o ineficientes que sean disparatadas y las excesivas que impliquen molestias innecesarias o humillaciones[166].

Seguidamente, dada su importancia, pasamos a analizar pormenorizadamente los requisitos de pertinencia, idoneidad y legalidad que ha de presentar cualquier prueba para que se estime procedente.

A. Pertinencia

El requisito de pertinencia se encuentra inmerso en el art. 24.2 CE al hacer mención expresa al mismo cuando establece que "todos tienen derecho […] a utilizar los medios de prueba pertinentes para su defensa".

---

[165] Así, el art. 25 del Estatuto de la Abogacía considera como infracción muy grave la revelación de datos o situaciones amparadas por el secreto profesional, con la consecuente sanción de suspensión del ejercicio de la profesión con un mínimo tres meses y un máximo dos años.
[166] DE URBANO CASTRILLO, E., *op. cit*., pp. 21-25.

Asimismo, se prevé en el art 281.1 LEC al disponer que "la prueba tendrá como objeto los hechos que guarden relación con la tutela judicial que se pretenda obtener en el proceso". Por tanto, "no deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente" (art. 283.1 LEC), es decir, no se aceptan pruebas irrelevantes o ajenas a la causa (sin ningún tipo de vinculación), o que no sirvan para probar el tema en cuestión, ya sea por tratarse de hechos admitidos de adverso o ya sea porque son notorios (art. 281, apartados 3 y 4, LEC).

De modo que la prueba electrónica será admitida, si es relevante para acreditar los hechos objeto del proceso, es decir, el *thema decidendi,* y para ello es necesario que previamente se hayan fijado los hechos sobre los que exista controversia entre las partes. En palabras de DELGADO MARTÍN, ha de existir una relación lógica entre el hecho que pretende acreditarse mediante el concreto medio probatorio y los hechos que constituyen el objeto de la convicción del juzgador[167] (pertinencia).

B. Idoneidad y necesidad

La idoneidad hace referencia a que el medio de prueba interesado sea conducente (útil) a efectos de acreditar algún hecho objeto del pleito, esto es, que su práctica sea precisa o indispensable.

Necesario, de acuerdo con DE URBANO CASTRILLO, es aquello que resulta obligado o forzoso para alcanzar un objetivo (probar un hecho controvertido). De modo que no se deben admitir pruebas que no favorezcan el esclarecimiento de la controversia, es decir, que sean inútiles (art. 283.2 LEC), tales como las superfluas o redundantes por no aportar nada nuevo al debate procesal.

[167] PICÓ I JUNOY, J.: *El derecho a la prueba en el proceso civil.* JM Bosch Editor, Barcelona, 1996, p. 45. Obra citada por DELGADO MARTÍN, J., *op. cit.*, p. 51.

C. Legalidad y licitud

De acuerdo con BUENO DE MATA[168], existe un tratamiento confuso en la doctrina y jurisprudencia por el uso de términos semejantes al referirse a la prueba ilícita. Por ello, es conveniente precisar la diferencia que encontramos entre prueba lega e ilícita.

Por un lado, la condición de la legalidad comporta que la práctica de la prueba sea acorde con los términos recogidos en la ley[169]. Se refiere al momento procesal oportuno de incorporación de un determinado medio de prueba pertinente dentro del proceso (legalidad procesal)[170].

Por otro lado, la licitud conlleva que el medio de prueba propuesto encaje (fuera del proceso) con los parámetros establecidos en la ley, de modo que no se practicará ninguna actividad probatoria contraria a la ley (art. 283.3 LEC). Así, cuando alguna de las partes entendiera que en la obtención u origen de las pruebas se han vulnerado derechos fundamentales, habrá de alegarlo de inmediato, dándose traslado a las demás partes. No obstante, la ilicitud de la prueba también podrá declararse de oficio por el juzgador o tribunal al tratarse de una materia de orden público (art. 287.1 LEC). Del mismo modo, el art. 11.1 LOPJ sanciona con la nulidad absoluta de las pruebas que se hayan obtenido violentando (directa o indirectamente) derechos o libertades fundamentales[171].

Según PICÓ I JUNOY, una prueba es lícita cuando no infringe ningún derecho fundamental ni en la obtención preprocesal del elemento probatorio, ni durante la práctica de la prueba del concreto medio de prueba, lo que necesariamente implica que se haya obtenido legalmente, que sea integral y no haya sido modificado ni alterado (esté intacto).

---

[168] BUENO DE MATA, F., *op. cit.*, p. 186.
[169] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 147.
[170] ILLÁN FERNÁNDEZ, J. Mª.: *La prueba electrónica, eficacia…, op. cit.,* p. 287. Obra citada por BUENO DE MATA, F., *op. cit.*, p. 188.
[171] Está nulidad se ha de extender a todas las pruebas que se hayan obtenido con razón de la anterior, en aplicación de la conocida doctrina del fruto del árbol envenenado o ponzoñoso, de creación jurisprudencial norteamericana.

La inalterabilidad del documento electrónico se garantiza mediante la aplicación de protocolos de extracción y copia, y mediante el adecuado manejo de las reglas de cadena de custodia[172].

3. Garantías que ha de reunir la prueba electrónica

A la hora de incluir en un proceso judicial una prueba electrónica, se deben tener en cuenta tres garantías.

- Autenticidad. Con esta garantía se hace énfasis en la autoría de la prueba electrónica. Así, del análisis del documento electrónico puede identificarse el dispositivo desde el que se ha confeccionado o remitido, no así quién lo ha materializado[173]. Por ello, de impugnarse su autenticidad se deberá aportar dictamen pericial informático o aquella prueba de cobertura que sea apropiada a tal efecto. No obstante, como ya hemos indicado, los documentos que estén oficialmente firmados mediante certificado electrónico gozan de certeza casi absoluta acerca de su autoría.

- Integridad. Esta garantía está expresamente prevista en el art. 383.2 LEC -en relación con el art. 384-, al disponer que "el material que contenga la palabra, la imagen o el sonido reproducidos habrá de conservarse por el Letrado de la Administración de Justicia, con referencia a los autos del juicio, de modo que no sufra alteraciones", garantizándose así la cadena de custodia.
  La importancia de salvaguardar esta garantía se debe a que la información que contiene un archivo digital es relativamente fácil de modificar, lo que puede suscitar grandes interrogantes acerca de su plenitud y manipulabilidad. Por ello, una buena forma de fundamentar la mismisidad[174] de la prueba

[172] Según Manuel RICHARD CONZÁLEZ, la cadena de custodia […] es el conjunto de actos que tienen por objeto la recogida, el traslado y la custodia de las evidencias obtenidas en el curso de una investigación criminal que tienen por finalidad garantizar la autenticidad, inalterabilidad e indemnidad de la prueba, en «La cadena de custodia en el proceso penal español», *Diario LA LEY* (8/11/2013). Disponible en: https://fdocuments.mx/document/wolters-kluwer-espana-sa-no-se-identifica-ley-especial-probatica-12pdf.html

[173] ORTUÑO NAVALÓN, Mª. C.: *La prueba electrónica ante los Tribunales.* Tirant lo Blanch, Valencia, 2014, p. 111. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 148.

[174] El ATS 2197/2012, de 9 de febrero, señalaba, en su FJ Segundo B), que el problema que plantea la cadena de custodia *"es garantizar que desde que se recogen los vestigios relacionados con el delito hasta*

electrónica es garantizando una correcta cadena de custodia mediante deposito notarial. De la misma manera, se puede realizar el peritaje informático en presencia de un notario que de fe de las operaciones que se realicen. Asimismo, éste podría proceder a la exploración directa de una página web o correo electrónico para confeccionar un acta a efectos de dar fe del contenido del mismo en ese momento.

El control de integridad o exactitud lo podemos realizar utilizando las siguientes técnicas[175]: i) Verificación del código secreto (PIN) de un determinado dispositivo de uso personal; ii) Desencriptación de documentos haciéndolos únicamente legibles para la persona que posee la clave de desciframiento[176]; y iii) Aplicación de técnicas de biometría, es decir, de tecnologías de identificación basadas en el reconocimiento de una característica física e intransferible de las personas[177].

- Licitud. El art. 287 LEC contempla el incidente de ilicitud probatoria que se sintetiza en las siguientes actuaciones[178]: a) Puede iniciarse de oficio o a instancia de parte; b) Se puede denunciar la ilicitud probatoria tanto en la obtención como en el origen de alguna prueba admitida; c) El incidente se

---

que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio de los juzgadores es lo mismo. Es a través de la corrección de la cadena de custodia como se satisface la garantía de la "mismidad" de la prueba. Se ha dicho por la doctrina que la cadena de custodia es una figura tomada de la realidad a la que tiñe de valor jurídico con el fin de en su caso, identificar en todo la unidad de la sustancia estupefaciente, pues al tener que pasar por distintos lugares para que se verifiquen los correspondientes exámenes, es necesario tener la ***completa seguridad de lo que se traslada, lo que se mide, lo que se pesa y lo que se analiza es lo mismo en todo momento, desde el instante mismo en que se recoge del lugar del delito hasta el fomento final en que se estudia y destruye****".*

[175] ABEL LLUCH, X.: "Prueba electrónica", ABEL LLUCH, X. y PICÓ I JUNOY, J. (directores). *La prueba electrónica*, Colección de Formación Continua de Derecho ESADE, J. M. Bosch editor, 2011, pp. 83-84. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 150.

[176] Así, por ejemplo, el sistema AES (*Advanted Encryption Standard*) -también llamado Rijndae- por el que se tardarían más de 2000 millones de años, utilizando un billón de ordenadores (que pudieran probar cada uno de ellos mil millones de claves por segundo), para descifrar una clave del sistema AES-128. *Vid*. "El algoritmo de encriptación AES, más vulnerable de lo que se creía", *El País*, 17/08/2011, disponible en: https://elpais.com/sociedad/2011/08/17/actualidad/1313532009_850215.html

[177] Por ejemplo, el reconocimiento facial o del patrón venoso del dedo y la lectura ocular de la retina, o incluso patrones de comportamiento como pueden ser escribir o caminar. Esta tecnología es óptima para la seguridad de equipos informáticos debido a la debilidad que pueden presentar contraseñas tales como "1234" o nombres conocidos. Vid. "Biometría, la tecnología que mide y analiza nuestros datos biológicos", *Iberdrola*. Disponible en: https://www.iberdrola.com/innovacion/ventajas-y-usos-biometria

[178] PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 156.

resuelve en el acto del juicio (si es ordinario), o en la vista antes de la práctica de la prueba (si es verbal); d) El Juzgador o Tribunal dará traslado a las partes para que se pronuncien acerca de la ilicitud de la prueba admitida; e) Podrán solicitar que se practiquen pruebas complementarias sobre la cuestión concreta de la ilicitud, admitiéndose las pertinentes y necesarias para dicho objetivo; f) El Juzgador o Tribunal resolverá oralmente sobre la ilicitud o no de la prueba; g) Contra dicha resolución oral cabrá interponer recurso de reposición, que se resolverá en el mismo acto, y contra la desestimación se podrá formular la oportuna protesta, a efectos de reproducir su impugnación en apelación.

Aparte de las anteriores garantías fundamentales, DE URBANO CASTRILLO[179] añade otra serie de pautas para pronunciarse acerca de la admisibilidad de las pruebas electrónicas. Estas son:

- Identificar propiamente el *hardware* o equipo del cual se origine el documento electrónico.
- Acreditar que dicho equipo informático opera correctamente, sin la intromisión de ningún tipo de *malware* (troyano o virus informático).
- Contrastar que el *software* refleja la exactitud de los datos introducidos en el proceso de registro del dispositivo electrónico.
- Deducir que el almacenamiento y la salida de datos se ha realizado de forma segura.
- Verificar la identidad de los participantes que han elaborado el documento electrónico.
- Constatar que en todo el proceso de elaboración se ha mantenido el control.

[179] DE URBANO CASTRILLO, E., "El documento electrónico: aspectos procesales", en LÓPEZ ORTEGA, J.J. (dir.), *Cuadernos de Derecho Judicial (Ejemplar dedicado a «Internet y derecho Penal»)*, núm. 10, Madrid, 2001, p. 589. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit*., p. 148.

4. Derecho comparado

A. Países de nuestro entorno:

a. Francia

La Ley 80/525, de 12 de julio de 1980, reforma el art. 1348 del Código Civil francés, consagrando implícitamente al documento electrónico el mismo valor probatorio que al documento en soporte material si reúne ciertos requisitos[180].

Así, en su Título III, Capítulo II, art. 1108-1 (introducido por la Ley nº2004-575, de 21 de junio de 2004, art. 25 Diario Oficial de 22 de junio de 2004), aclara que en los actos jurídicos en los que sea necesaria la escritura para constituir los mismos, podrá hacerse de forma electrónica, en concordancia con los arts. 1316-1 y 1316-4 y, si se requiere un acta de formalización, igualmente se podrá elaborar de manera informatizada, de acuerdo con el art. 1317[181].

Asimismo, el art. 1316 (Capítulo VI, de la prueba de obligaciones y del pago, Sección I, de la prueba documental) indica que el contrato electrónico será admitido como prueba, al igual que si fuera manuscrito, siempre y cuando cumpla las condiciones de autenticación y conservación que garanticen su seguridad (apartado 1). Con ello se dota con la misma fuerza probatoria al documento en soporte papel y electrónico[182].

Por su parte, la reforma de la Ley nº2000-230, de 13 de marzo de 2000, sobre la adaptación al derecho de la prueba a las nuevas tecnologías de la informática, en relación con la firma electrónica, dispone en su art. 1316 que "la prueba literal, o prueba por escrito, resulta de un seguido de letras, caracteres, cifras o todo otro signo o símbolo dotados de significado inteligible, cualquiera que sea su soporte y sus modalidades de transmisión". Con ello, se incorporan los soportes informáticos dentro de las pruebas documentales. Además, añade el apartado 1 de este artículo que el documento escrito con

---

[180] PALADELLA SALORD, C.: "El documento electrónico como prueba. La reforma del Código Civil Francés", *Revista Electrónica de Derecho Informático*, nº26, de septiembre 2000. Obra citada por AIGE MUT, Mª B, *op. cit*., pp. 58 y 59.
[181] *Ibídem*, pp. 59 y 60.
[182] *Ibídem*, pp. 60 y 61.

en soporte electrónico será admitido como prueba y con la misma validez y eficacia que el presentado en soporte papel[183].

Para terminar, es de subrayar que el Código Civil francés, en su art. 1322, otorga a la escritura privada reconocida el mismo valor que a una escritura pública. Esto se traduce en la posibilidad de conceder a los documentos privados -y, por ende, a los electrónicos- el valor de prueba tasada, a diferencia de lo que sucede en la legislación española, en la que predomina el libre y sano criterio del juzgador[184].

b. Alemania

De acuerdo con la Ley procesal civil alemana, *Zivilprozessordnung* (en adelante, ZPO) documento es la corporación escrita del pensamiento humano, por lo general en formato papel o similar (§ 415 a 444 ZPO). Por tanto, no se incluyen en tal definición los documentos electrónicos porque únicamente son legibles o perceptibles a través de un dispositivo electrónico[185], al no ser su naturaleza corpórea y variar su ubicación.

No obstante lo anterior, Alemania es una nación que ha tenido en cuenta el comercio electrónico desde su surgimiento, por lo que en 2001 incorporó la forma electrónica como fuente de prueba válida en su Código Civil, *Bürgerliches Gesetzbuch* (en adelante, BGB)[186]. Con ello, la *"forma escrita puede ser reemplazada por una forma electrónica, a menos que un estatuto lleve a una conclusión diferente"* (§ 126 BGB).

En cuanto a su eficacia procesal, el § 371 ZPO incorpora el documento electrónico como objeto susceptible de reconocimiento judicial para presentarse como una prueba en un proceso. Por tanto, su medio de prueba sería el reconocimiento judicial y no la documental, a no ser que este estuviera autentificado mediante una firma electrónica cualificada o reconocida, teniendo entonces el tratamiento de documento privado (o hubiera sido expedido por una autoridad pública, aplicándole las normas previstas para

[183] *Ibídem*, p. 59.
[184] *Ibídem*, p. 61.
[185] Como señalan BALZER o GEIS, ambos citados por ORMAZÁBAL SÁNCHEZ, G.: "La prueba mediante documento electrónico digitalmente firmado", *Actualidad Civil, nº1*, 1999, pp. 219-234. Obra citada por AIGE MUT, Mª. B., *op. cit*., p. 51.
[186] *Ibídem*, p. 52.

los documentos públicos). En estos casos, según el § 416, los documentos privados electrónicos con firma electrónica reconocida harán prueba plena de las declaraciones que se contienen[187].

c. Italia

En el Derecho italiano, el Decreto de la Presidencia de la República (en adelante, DPR) de 10 de noviembre de 1997, para el desarrollo del art. 15.2 de la Ley de 15 de marzo de 1997, ya hacía referencia al régimen de formación, archivo y transformación del documento informático y telemático. Así, lo definía como la representación en forma informática o electrónica de actos, hechos o datos jurídicamente relevantes [art. 1.a)] que es eficaz y válido a todos los efectos legales (art. 2). En la actualidad, este decreto fue derogado por el Decreto 445/2000, de 28 de diciembre, el cual acoge la misma definición en su art. 1.b)[188].

De esta manera difiere del Derecho alemán, porque por regla general considera que forman parte de la naturaleza de los documentos escritos. Por ello, los arts. 2702 y 2712 del Código Civil Italiano estipulan que los documentos electrónicos son pruebas válidas con los mismos efectos jurídicos que los documentos privados. Por lo tanto, son asimilables a los documentos tradicionales o en formato papel, siendo un tipo de *sui generis* de documento escrito[189]. Asimismo, el art. 2712 indica que la reproducción fotográfica, informática o cinematográfica, el registro fonográfico y, en general, cualquier otra reproducción mecánica de hechos y cosas, son pruebas plenamente válidas.

Dicho artículo fue modificado por un Decreto de 7 de marzo de 2005, relativo al Código de la Administración Digital. Este resalta la definición que hace en su art. 1.1.p) de documento informático. Así, precisa que es aquella representación informática de actos, hechos o datos jurídicamente relevantes, asemejándose de esta manera a los documentos clásicos, diferenciándose únicamente por su soporte material[190].

[187] *Ibídem*, p. 53.
[188] *Ibídem*, p. 55.
[189] *Ibídem*, p. 56.
[190] *Ibídem*, pp. 57 y 58.

También resalta en este Decreto, el Capítulo II, Sección I, sobre el Documento Informático, en concreto el art. 20, el cual dispone que el documento informático, independientemente de su formato, registro y transmisión, es válido y relevante a efectos jurídicos. Además, si cuentan con firma electrónica cualificada o certificado digital, cumplen con el requisito legal de la forma escrita.

Sobre su valor probatorio, el art. 21 establece que el documento informático validado con una simple firma electrónica será valorado libremente por el juzgador, de acuerdo a sus características objetivas de seguridad y calidad. Por el contrario, si está suscrito con certificado digital o firma electrónica cualificada, tendrá la eficacia de los arts. 2702 de Código Civil, es decir, documental privada.

Por su parte, el Código de Procedimiento Civil, establece en su artículo 261 del § IX, sobre la inspección, reproducción mecánica y experimentos -del Libro Segundo, relativo al proceso con carácter general (*Processo di Cognizione*)- que el juzgador puede disponer que se efectúen reproducciones de fotografías de objetos, documentos y lugares, o reproducciones cinematográficas y otras que exijan el empleo de medios, instrumentos o procedimientos mecánicos[191].

B. Derecho latinoamericano:

a. Colombia

En Colombia la Ley 527 de 1999 promulga, en su artículo 5º, que no se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté en forma de mensaje de datos.

Ahí, al igual que aquí, se reconoce a las partes el principio de contradicción de la prueba y, consiguientemente, la libre valoración del juez. Sin embargo, en este país, al derivar gran parte de su derecho penal del estadounidense, contrastan en ese proceso, ya que el vocablo "evidencia" (*evidence*) se distingue del de "prueba" (*proof*), como

[191] *Ibídem*, p. 57.

elemento de convicción para la emisión de un fallo, a diferencia de nuestro sistema procesal, en el que estos vocablos son completamente sinónimos.

Por lo demás, el tratamiento de la prueba electrónica en el proceso civil colombiano es prácticamente igual que el español, ya que su aportación está condicionada a cumplir con los principios de legitimación, inmaculación, conducencia, legalidad, licitud, pertinencia, oportunidad y utilidad[192], que se pueden sintetizar e integrar en los que hemos expuesto anteriormente.

b. Bolivia

El Código Procesal Civil Boliviano -promulgado por la Ley 439, de 19 de noviembre de 2013- (en adelante, CPCB) reconoce, en su artículo 144.II, como medios de prueba, entre otros, "los documentos y firmas digitales y los documentos generados mediante correo electrónico"[193]. Sin embargo, al igual que la LEC, el CPCB no contiene una definición de prueba o documento electrónico[194], ni tampoco una regulación específica para la aportación y admisión de pruebas electrónicas, por lo que se somete de manera analógica y confusa a las reglas convencionales de las pruebas tradicionales (art. 148.III CPCB), con el mismo rango y amparo constitucional que cualquier prueba, envuelto en el derecho fundamental a la tutela judicial efectiva.

Como ejemplo de la confusión que se da en Bolivia con este tipo de pruebas, ÁVILA GONZÁLEZ nos pone el caso del acceso de los documentos tradicionales al proceso. Así, en el CPCB las disposiciones procesales sobre la carga de la prueba obligan a las partes a aportar los documentos originales con la demanda en el plazo establecido para ello (art.111.I), con apercibimiento de llegar a ser inadmisibles por su defectuosidad

---

[192] NISIMBLAT, NATTAN: "El manejo de la prueba electrónica en el proceso civil colombiano". Universidad de los Andes. Facultad de Derecho. Revista Nº4 (2010), pp. 3-5. URL: file:///C:/Users/UPEGUI/Downloads/Dialnet-ElManejoDeLaPruebaElectronicaEnElProcesoCivilColom-7507234.pdf

[193] ÁVILA GONZALEX, N.: "Las capturas de pantalla como medio de prueba en el proceso civil". *Rev. Boliv. de Derecho Nº27*, enero 2019, pp. 274 y ss. Disponible en: http://www.revista-rbd.com/articulos/2019/27/272-295.pdf

[194] Si bien, la Ley General de Telecomunicaciones boliviana contiene en su artículo 6.IV.4 una definición de documento digital, del siguiente modo: "toda representación digital de actos, hechos o datos jurídicamente relevantes, con independencia del soporte utilizado para su fijación, almacenamiento o archivo".

(art. 112.I). Sin embargo, respecto de los documentos electrónicos, el art. 148.III del CPC considera los considera fuente de prueba, en contradicción a lo establecido en el art. 144.II, que los concibe como un 'medio' de prueba autónomo, evidenciándose con ello -como destaca la autora- la confusión generada por la omisión en la distinción entre fuente y medio de prueba que se produce en la legislación del procedimiento civil boliviano, al igual que ocurre en el español cuando en el art. 299 LEC utiliza para referirse a las fuentes de prueba el término "medio".

Estas similitudes que se presentan entre ambas normas procesales se debe -de acuerdo con la referida autora- a que el legislador boliviano ha reproducido casi con exactitud los desaciertos del legislador español en la LEC. Por lo demás, al igual que pasa con la legislación colombiana, este sistema procesal civil no difiere mucho del español respecto al tratamiento que tiene en ellos la prueba electrónica.

c. Ecuador

En nuestra materia, resulta interesante la lectura del art. 1715 del Código Civil ecuatoriano, en el cual se enumeran los medios de prueba, entre los que encontramos los «instrumentos» públicos y privados. Nos llama mucho la atención la utilización de este término, ya que a diferencia de nuestra legislación y las de nuestro entorno, que utilizan el concepto de documento, parece que la Ley boliviana está más avanzada en este sentido al ser el concepto de instrumento que utiliza más amplio y, por tanto, poder incluirse en este los documentos informáticos y así someterse a la valoración judicial de su art. 1719 (que resulta análoga a la sana crítica del juzgador acogida por nuestro derecho)[195].

A su vez, el art. 125 del Código de Procedimiento Civil ecuatoriano enumera también y de la misma manera los medios o «instrumentos» probatorios, pero, a diferencia de la LEC, no incluye en su lista los soportes electrónicos. Es más, define en su art. 195 los instrumentos privados, precisando únicamente que sean hechos por los particulares.

[195] AIGE MUT, Mª. B., *op. cit.*, pp. 63 y 64.

Con lo cual, deja la puerta abierta a una posible correspondencia entre los soportes tradicionales y los informáticos.

Por su parte, la Ley de Comercio Electrónico de Ecuador, equipara en su art. 2 los efectos jurídicos de los documentos electrónicos a los manuscritos. Asimismo, su art. 51 incluye los instrumentos públicos electrónicos, otorgándoles en el siguiente artículo, el mismo valor probatorio previsto para los mismos en el Código de Procedimiento Civil[196].

Finalmente, podemos notar que la legislación de los países latinoamericanos tiende a ser flexible de una manera u otra en cuanto a la aceptación y valoración de los documentos en soporte electrónico. Así, en México existe una Ley de Firma Electrónica Avanzada desde 2012, la cual facilita los servicios online; en Chile el Decreto 81 otorga ciertos efectos jurídicos a los documentos electrónicos para su validez procesal; en Perú se regula la figura del fedatario informático, que da fe de conocimientos acerca de las tecnologías de la información para garantizar su seguridad (Decreto Legislativo nº681, de 1991); y en Costa Rica se encuentra la Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos[197].

VII. IMPUGNACIÓN Y VALORACIÓN DE LOS MEDIOS PROBATORIOS DIGITALES

1. Impugnación de las pruebas electrónicas aportadas (art. 326 LEC)

La finalidad del trámite "impugnatorio" queda anticipada en la EM de la LEC al afirmar que *"la Ley pretende que cada parte fije netamente su posición sobre los documentos aportados de contrario, de suerte que, en caso de reconocerlos o no impugnar su autenticidad, la controversia fáctica desaparezca o quede aminore"*.

Los reconocidos ABEL LLUCH y PICÓ JUNOY, entienden en esta sede por impugnación, la facultad de realizar alegaciones o de aportar medios de prueba que

[196] *Ibídem*, p. 64
[197] *Ibídem*, p. 65

desvirtúen el contenido de una prueba electrónica de adverso[198], pudiendo realizarse en los mismos momentos procesales oportunos que el resto de pruebas, esto es, en la audiencia previa[199] o diligencias finales -en el juicio ordinario-, o en el acto de vista en el juicio verbal[200].

Se trata de un "posicionamiento" sobre los documentos materiales (art. 265 LEC), no sobre los procesales (art. 264 LEC), pudiendo este posicionamiento desplegarse a partir de una triple posición: 1º) reconocer el documento: la otra parte lo reconoce como auténtico y, asimismo, suscrito por ella; 2º) admitir el documento: la contraparte no lo ha suscrito, pero reconoce su autenticidad; y 3º) impugnar la autenticidad, exactitud o ilícitud del documento: el adversario considera que no es auténtico o la copia, certificación o testimonio no es exacto o se ha obtenido vulnerando derechos fundamentales, y decide impugnarlo[201].

En el trámite de posicionamiento[202] se podrá impugnar la "autenticidad" y la "exactitud" del documento y en la valoración en sentencia el juez deberá comprobar la

---

[198] ABEL LLUCH, X. y PICO JUNOY, J.*: La prueba electrónica*, J. Mª Bosch editor, Barcelona, 2011, pp. 178 a 195. Obra citada por VERGÉS CORTIT, R., *op. cit*., p. 214.

[199] El artículo 427 LEC, en sede de audiencia previa del juicio ordinario, alude al "posicionamiento" sobre documentos en los términos literales siguientes: "*En la audiencia previa, cada parte se pronunciará sobre los documentos aportados de contrario hasta ese momento, manifestando si los admite o impugna o reconoce o si, en su caso, propone prueba acerca de su autenticidad".*

[200] VERGÉS CORTIT, R., *op. cit*., p. 214.

[201] MIRA ROS, C., *El expediente electrónico*, ed. Dykinson, Madrid, 2010, p.18-19 atribuye al documento electrónico las siguientes características: 1ª) La grafía binaria; 2ª) La inmaterialidad del documento electrónico; y 3ª) La ausencia de firma manuscrita. Obra citada por ABEL LLUCH, X., en "La impugnación de la prueba electrónica". *Justicia: revista de derecho procesal*, 2019, pp. 225 y 226.

[202] La SAP de Barcelona, de 11 de octubre de 2017 (Roj: SAP 9677/2017), ilustra el alcance y los efectos valorativos del llamado «posicionamiento» ante documento cuando en su FJ Tercero, dispone que: *"El documento contable a que venimos refiriéndonos, en contra de lo que se afirma en la sentencia, no fue impugnado por la parte demandada por la sencilla razón de que ésta no compareció al acto de la audiencia previa, que es el momento en el que las partes pueden posicionarse sobre la documentación aportada por la contraria (artículo 427 de la Ley de Enjuiciamiento Civil), y en virtud de ese posicionamiento, arbitrar la oportuna prueba necesaria para la acreditación de los hechos por ellas alegados. No se hizo así por la parte demandada. Pero es que, aun en el caso de que se hubiese hecho, en los términos indicados en la contestación a la demanda (impugnó el documento por haber sido elaborado por la parte contraria por lo que, según dijo, carece de valor probatorio), esa impugnación no habría tenido el efecto pretendido por la parte demandada. Conforme con lo dispuesto en los artículos 326 y 316 de la Ley de Enjuiciamiento Civil y la jurisprudencia que los interpreta, el hecho de impugnar un documento privado no le priva de valor probatorio, sino que faculta al proponente a proponer otra prueba añadida que contribuya a confirmar la autenticidad (veracidad) del documento (cotejo de letras, o proponer cualquier otro medio útil y pertinente al efecto). Si de la prueba complementaria resulta la autenticidad, el documento hace prueba plena, y las costas, gastos y derechos que origine el cotejo o comprobación serán de cargo de quien hubiese formulado la impugnación, pero si dicha prueba complementaria no da resultado o no ha se ha propuesto prueba alguna, el documento podrá ser valorado por el Juez según las reglas de la sana crítica, es decir, podrá*

"certeza" del documento, mediante la valoración del documento "impugnado" (en su contenido) junto con las restantes pruebas obrantes en las actuaciones[203].

Siguiendo a DELGADO MARTÍN[204], en el proceso civil, la falta de impugnación por aquel a quien perjudica comportaría un supuesto de prueba tasada: de modo que el documento hará prueba plena en los mismos términos que los documentos públicos (art. 326.1 LEC).

Por el contrario, en caso de impugnación por alguna de las partes, el órgano judicial valorará la autenticidad e integridad conforme a las reglas de la sana crítica, ponderando las alegaciones en que se fundamenten los motivos de impugnación (art. 384.1 LEC *in fine*) y los medios de prueba y dictámenes periciales propuestos (art. 382.2 por remisión del art. 384.2 LEC)[205].

Como anteriormente se ha indicado, a diferencia de las pruebas tradicionales o clásicas, la prueba digital es, en su esencia, intangible, ya que su naturaleza es virtual, lo que puede suponer un reto para distinguir los archivos originales de las copias, siendo mejor en muchas ocasiones acreditar que la prueba aportada al proceso no está modificada (o contiene "vicios ocultos") a través de garantías y protocolos procesales, con la finalidad de así eludir su posible impugnación fundada en su inexactitud o falsedad.

Así, ORTUÑO NAVALÓN[206] compara la impugnación entre documento tradicional y electrónico, dándonos las siguientes notas:

- En el documento tradicional podemos impugnar tres cuestiones básicas: i) la autenticidad, esto es, la concordancia entre el autor aparente y el real; ii) la exactitud, que es la correspondencia entre el original y la copia, testimonio o certificación; y iii) la certeza, es decir, la congruencia entre las declaraciones

ser libremente valorado. De otro modo, quedaría al arbitrio de la parte contraria la eficacia probatoria de los documentos aportados por la contraria".

[203] ABEL LLUCH, X.: "La impugnación de la prueba electrónica". *Justicia: revista de derecho procesal*, 2019, p. 228.

[204] DELGADO MARTÍN, J., *op. cit*., p. 83.

[205] *Ibídem*, p. 84.

[206] ORTUNO NAVALÓN, Mª. C.: *La prueba electrónica ante los Tribunales*. Tirant lo Blanch, Valencia, 2014, p. 110. Obra citada por PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C., *op. cit.*, p. 147.

contenidas en el documento y la realidad, que cuando se trate de un archivo digital, se podrá impugnar su contenido (dadas sus características) igualmente en fase de conclusiones, cuando se proceda a valorar la prueba conjunta practicada en el juicio[207].

- En el documento electrónico, aparte de los tres aspectos anteriores, pueden añadirse otros tres motivos impugnatorios: a) la integridad, o sea, que el soporte en el que se presente no haya sido alterado; b) la correspondencia entre la realidad del sujeto al que se atribuye y el contenido que refleja; y c) la licitud, que supone que en su obtención no se haya violentado derechos o libertades fundamentales.

Precisamente, si se suscitan interrogantes acerca de la veracidad de los archivos digitales, la parte que los haya aportado tendrá que proponer todas aquellas pruebas pertinentes y útiles que demuestren su autenticidad[208] (el llamado cotejo pericial de letras). En la práctica es frecuente manifestar la falta de reconocimiento del documento privado por la parte no lo ha propuesto, ya que, de lo contrario, su reconocimiento expreso tiene todo su contenido el valor de prueba plena en el proceso. Además, si el documento no es impugnado expresamente la valoración judicial tenderá a presumir su autenticidad, salvo prueba en contrario o manifiesta falsedad.

Si se tratare de documento públicos, en principio no son susceptibles de impugnación y se tienen que tener como probados, a no ser que existan claros indicios de que se trata de documentos falsificados, por lo que si se presenta una copia se requerirá el cotejo con el original (matriz notarial si se trata de una escritura pública) o si se presenta el original se requerirá la ratificación del funcionario que elaboró dicho documento[209].

A modo de ejemplo reiterativo, podríamos acudir al cotejo del LAJ o al reconocimiento judicial del soporte en que se halla originalmente el documento

---

[207] VERGÉS CORTIT, R., *op. cit.*, p. 215.
[208] DE PRADA RODRÍGUEZ, M.: *op. cit.*, p. 345
[209] ROJAS ROSCO, R.: "La prueba digital en el ámbito laboral ¿son válidos los "pantallazos"? en *La prueba electrónica…op. cit*., p. 94.

electrónico. Asimismo, podemos instar el acta notarial, la pericial informática o, mismamente, la ratificación del autor o destinatario. Del mismo modo se podría contrastar con el interrogatorio de parte o de una persona (física o jurídica).

Finalmente, recalcar que cabe realizar la impugnación de las pruebas electrónicas en segunda instancia (siempre que la sentencia no sea firme) mediante la interposición del recurso ordinario de apelación o el extraordinario por infracción procesal, además de la revisión de la sentencia firme, pudiendo ser revisada la misma de manera íntegra por el órgano superior[210], ya que la valoración de este tipo de pruebas está sujeta a las reglas de la sana crítica y máximas de la experiencia, lo cual supone una excepción al veto que la jurisprudencia viene estableciendo sobre la posibilidad de sustituir el criterio objetivo e imparcial de los Jueces de instancia[211].

2. Valoración de la prueba electrónica por parte del Juzgador

El procedimiento probatorio de la prueba electrónica culmina con la valoración conjunta del material probatorio[212]. Siguiendo a DELGADO MARTÍN[213], la valoración de la prueba significa otorgarle la credibilidad que merece de conformidad con el sistema de valoración establecido por el legislador, que puede ser tasado o libre. Así, nuestro legislador ha optado por la libre valoración de la prueba por parte del órgano judicial, frente al sistema de prueba legal o tasada (como ocurre con los llamados documentos públicos)[214]:

- Las pruebas legales son aquellas que la ley señala previamente el grado de eficacia que se le debe atribuir por parte del juzgador a determinado medio probatorio.
- En el sistema de libre, el Juez o Tribunal motiva la valoración discrecionalmente junto con las reglas del criterio racional.

---

[210] VERGÉS CORTIT, R., *op. cit.*, p. 215.
[211] SEVILLA CÁCERES, F.: "Valoración de la prueba por el Tribunal de apelación". *Mundo jurídico.info*. Disponible en: https://www.mundojuridico.info/valoracion-de-la-prueba-por-el-tribunal-de-apelacion/
[212] DE URBANO CASTRILLO, E*: La valoración de…op. cit.*, p. 25.
[213] DELGADO MARTÍN, J., *op. cit*., p. 77.
[214] *Ibídem*, p. 78.

Así, la regulación de la valoración de la prueba electrónica se contiene en el apartado 3 del art. 382, al señalar que *"el tribunal valorará las reproducciones […] según las reglas de la sana crítica"*, y en el apartado 3 del art. 384, ambos de la LEC[215], por lo que, a diferencia de los medios probatorios legales o tasados, la valoración de la prueba electrónica queda expuesta al criterio del juzgador.

Por tanto, hemos de concluir que, en España, la valoración de la prueba electrónica es general y en su conjunto, sin que prevalezca unas pruebas sobre otras (salvo los supuestos de documento público), por lo que depende únicamente del sano y libre criterio del juzgador[216].

Si bien, esta valoración no implica una prueba arbitraria, sino que es una valoración discrecional basada en las reglas de la sana crítica, máximas de la experiencia, conocimiento privado del juez y, por supuesto, la correspondiente motivación de los referidos criterios (cuando se den). Así, mientras que una parte presenta un documento manuscrito a lápiz de borrar (lo que lo haría aún más fácil de manipular), si la otra parte no lo impugna, se admitirá por el Juzgador o Tribunal. En cambio, si lo que se presenta es el mismo texto escrito a ordenador, si no lo incluyéramos como prueba documental, este podría ser valorado libremente por el órgano judicial[217].

Entonces, la pregunta que nos surge es qué pasa cuando al aportarse en un proceso judicial un medio de prueba electrónico, el juzgador cuestiona la originalidad o inmaculación, esto es, la forma en la que fue recolectada, procesada, copiada o manipulada, o bien duda sobre la constitucionalidad de su obtención.

La mencionada hipótesis se prevé en el art. 334 LEC -rubricado como "Valor probatorio de las copias reprográficas y cotejo"-, al disponer en su apartado uno*: si la parte a quien perjudique el documento presentado por copia reprográfica impugnare la*

---

[215] Este último artículo, que se encabeza con el título "De los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso", manifiesta, en el aludido apartado, que *el tribunal valorará los instrumentos […] conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza.*
[216] DE URBANO CASTRILLO, E*: La valoración de…op. cit.*, pp. 28 y 29.
[217] AIGE MUT, Mª. B.: *Los documentos electrónicos en el ámbito del proceso.* Aranzadi, Pamplona, 2015, p. 103.

exactitud de la reproducción, se cotejará con el original, si fuere posible y, no siendo así, se determinará su valor probatorio según las reglas de la sana crítica, teniendo en cuenta el resultado de las demás pruebas.

VIII. CONCLUSIONES

Como primera conclusión, podemos extraer la falta de una regulación específica y detallada de las pruebas electrónicas, así como la gran ventaja que existe entre el mundo tecnológico -que, fabulosamente, podría ser la liebre- y el derecho vigente -que, sin duda, es la tortuga-, lo que consecuentemente acarrea una disminución en la seguridad jurídica, especialmente en atención al derecho fundamental de tutela judicial efectiva del artículo 24 CE, del que deriva el derecho a la práctica de la prueba solicitada.

Por lo anterior y por lo complicado que a veces resulta presentar este tipo de pruebas al Juzgador o Tribunal, es práctica habitual que se exijan más garantías que con otras pruebas.

Si bien, como hemos visto, está empezando a haber un gran repertorio de jurisprudencia de referencia (en todos los órdenes jurisdiccionales) que profundiza acerca de la validez y los requisitos que ha de presentar la prueba electrónica, lo que siempre es de gran ayuda. Aunque también es cierto que en cualquier momento pueden cambiar tales criterios jurisprudenciales.

Estos hipotéticos cambios, pudieran tener su razón en lo tecnicista que es la materia en cuestión -que requiere un conocimiento adecuado para que no se comentan fraudes o injusticias, aprovechándose de ello alguna de las partes-, además de mucha práctica y actualizaciones continuas, que vayan a la par de los constantes avances que se producen en el mundo de las TIC.

Por otro lado, es de destacar, que la prueba electrónica puede ofrecernos información fidedigna y objetiva, en comparación con otras pruebas tradicionales como puede ocurrir en la testifical, siempre subjetivada, o la documental manuscrita, muy volátil y expuesta a sufrir alteraciones y refutaciones. Se trata, pues, de una prueba idónea

que con el debido uso acredita una serie de hechos que antes no se podían acreditar por el desconocimiento y obsolescencia de las TIC.

Asimismo, hoy en día su obtención, uso y almacenamiento suele resultar una tarea sencilla, que para la mayoría de nuestra sociedad apenas requiere de medios de difícil alcance o arduos conocimientos. Un ejemplo claro de esto es la posesión de un *pen drive*, en el cual se pueden albergar miles de datos que incluso se pueden proteger de manera cifrada mediante el uso de contraseñas o sistemas de encriptación, lo que cualquiera puede aprender a hacer si no lo sabe ya, viendo un simple tutorial en YouTube, en donde prácticamente podemos aprender a hacer cualquier cosa que se nos pase por la cabeza, algo que un buenas manos ayuda y, por el contrario, en las no indicadas es un riesgo, el cual conlleva el uso de Internet, esa red dónde se comparten conocimientos y bulos.

En definitiva, debido a que esta es una materia con una regulación que se podría decir que es un tanto imprecisa o indeterminada -o, por el contrario, dispersa, con puntos de vista en la doctrina opuestos-, la misma requiere de mucha prudencia y crítica, tanto por los profesionales de la abogacía, ya que el mismo cliente nos puede mostrar (a sabiendas o no) datos electrónicos manipulados por él mismo o un tercero, y nosotros caer en esa falacia y probablemente también al juzgador, con la oportuna injusticia que se cometería. Por ello y por lo usual que se está volviendo la utilización de este tipo de pruebas, es muy conveniente el conocimiento y estudio de la presente obra, la cual nos proporciona medios adecuados tanto de defensa como de fuerza para refutar o acreditar, respectivamente, hechos electrónicos de toda índole.

IX. JURISPRUDENCIA

- Auto de la Sala de lo Penal del Tribunal Supremo, de 9 de febrero de 2012 (Roj: ATS 2197/2012)
- Sentencia de la Sala de lo Penal del Tribunal Supremo, de 19 de mayo de 2015 (Roj: STS 300/2015)
- Sentencia de la Sala de lo Penal del Tribunal Supremo, de 27 de noviembre de 2015 (Roj: STS 5421/2015)
- Sentencia de la Sala de lo Penal del Tribunal Supremo, de 10 de diciembre de 2015 (Roj: STS 5809/2015)
- Sentencia de la Sala de lo Civil del Tribunal Supremo, de 19 de noviembre de 2018 (Roj: STS 3904/2018)
- Sentencia de la Sala Segunda del Tribunal Constitucional, de 29 de noviembre de 1984 (Roj: STC 114/1984)
- Sentencia del Pleno del Tribunal Constitucional, de 19 de noviembre de 2020 (Roj: STC 172/2020)

- Sentencia de la Audiencia Provincial de Barcelona (Sección 13), de 2 de mayo de 2007 (Roj: SAP B 4399/2007)
- Sentencia de la Audiencia Provincial de Cuenca (Sección 1) de 30 de junio de 2009 (Roj: SAP CU 301/2009)
- Sentencia de la Audiencia Provincial de Santa Cruz de Tenerife (Sección 4) de 27 de marzo de 2012 (Roj: SAP TF 512/2012)
- Sentencia de la Audiencia Provincial de Pontevedra (Sección 3) de 31 de mayo de 2017 (Roj: SAP PO 1081/2017)
- Auto de la Audiencia Provincial de Barcelona (Sección 13) de 15 de enero de 2018 (Roj: AAP B 15/2018)
- Sentencia de la Audiencia Provincial de Baleares (Sección 3) de 8 de noviembre de 2018 (Roj: SAP IB 2071/2018)
- Sentencia de la Audiencia Provincial de Pontevedra (Sección 3) de 13 de junio de 2018 (Roj: SAP PO 1302/2018)
- Sentencia [Penal] de la Audiencia Provincial de Madrid (Sección 27) de 20 de septiembre de 2018 (Roj: SAP M 15080/2018)

X. BIBLIOGRAFÍA

- A. R.: "El algoritmo de encriptación AES, más vulnerable de lo que se creía", *El País* (17/08/2011). URL: https://elpais.com/sociedad/2011/08/17/actualidad/1313532009_850215.html
- ABEL LLUCH, X.: "La impugnación de la prueba electrónica". *Justicia: revista de derecho procesal*, 2019
- AIGE MUT, Mª. B.: *Los documentos electrónicos en el ámbito del proceso*. Aranzadi, Pamplona, 2015
- ARMENTA DEU, T.: "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre". IDP. Revista de Internet, Derecho y Política, Universidad de Girona, 2018. URL: https://www.raco.cat/index.php/IDP/issue/view/28731/125
- ARRABAL PLATERO, P: *La prueba tecnológica: aportación, práctica y valoración.* Tirant lo blanch, Valencia, 2020.
- ASENCIO MELLADO, J. Mª.: *Derecho Procesal Civil. Parte General*. Tirant lo blanch, Valencia, 2019
- ÁVILA GONZALEX, N.: "Las capturas de pantalla como medio de prueba en el proceso civil". *Rev. Boliv. de Derecho Nº27*, enero 2019. URL: http://www.revista-rbd.com/articulos/2019/27/272-295.pdf
- BELLOCH ORTÍ, C.: "Las Tecnologías de la Información y Comunicación". Universidad de Valencia. URL: https://www.uv.es/~bellochc/pdf/pwtic1.pdf
- "Biometría, la tecnología que mide y analiza nuestros datos biológicos", Iberdrola. Disponible en: https://www.iberdrola.com/innovacion/ventajas-y-usos-biometria
- BUENO DE MATA, F.: *Prueba electrónica y proceso 2.0*. Tirant lo blanch, Valencia, 2014
- "BuroSMS y SMS (e-Mensajes)", *Consejo General de la Abogacía Española* (CGAE). URL: https://www.abogacia.es/servicios/abogados/burosms/
- CALLEJO, ALBER: "Así funciona el nuevo Modo Centinela que ha desarrollado Tesla para evitar robos". *Forococheselectricos* (16/02/2019). URL:

https://forococheselectricos.com/2019/02/asi-funciona-el-nuevo-modo-centinela-que-ha-desarrollado-tesla-para-evitar-robos.html

- COLOMA CORREA, R. (2020): "La prueba y sus significados". *Revista Chilena de Derecho*, vol. 46 Nº 2. URL: http://tallerdeletras.letras.uc.cl/index.php/Rchd/article/view/9618/8976
- CONSEJO GENERAL DEL NOTARIADO: "Actas notariales" [consultado el 6 de enero de 2021]. URL: https://www.notariado.org/portal/actas-notariales
- DE PRADA RODRÍGUEZ, M. y VVAA: *Nuevos horizontes del derecho procesal*. J.M. Bosch Editor. Barcelona, 2019
- DE URBANO CASTRILLO, E.: *La valoración de la prueba electrónica*. Tirant lo blanch, Valencia, 2009
- DELGADO MARTÍN, J.: *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Wolters Kluwer, Madrid, 2016
- "¿Dónde guarda y almacena Skype las: Fotos, archivos, conversaciones y grabaciones?". *Mira Cómo Se Hace* (26/03/2020). Disponible en: https://miracomosehace.com/donde-guarda-almacena-skype-fotos-archivos-conversaciones-grabaciones/
- ESPINÓS, ENRIQUE: "¿Puedo usar una cámara on board para denunciar a otro conductor?". Autofácil. URL: https://www.autofacil.es/legal/2019/05/23/camara-on-board-denunciar-conductor/50382.html
- FLORES HERRERA, J.: "Qué Es HTML". *Códigofacilito*. URL: https://codigofacilito.com/articulos/que-es-html
- GALISTEO, ALEJANDRO: "Te pueden desahuciar si subalquilas sin permiso un piso en Airbnb". *Expansión* (31/12/2020). URL: https://www.expansion.com/juridico/sentencias/2020/12/31/5fdc8967e5fdead32e8b4659.html
- GAMELLA CARBALLO, S.: Redes sociales y otros medios de prueba digital: WhatsApp, Facebook, Twitter, Skype, correo electrónico, Google Maps, GPS y cámaras de videovigilancia. Sepín (Selección de Jurisprudencia), Madrid, 2019
- GASTÓN E. BIELLI.: "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática". *E-procesal.com* (03/06/2019). URL: http://e-procesal.com/dterceros-de-confianza-y-

certificacion-de-prueba-electronica-una-nueva-frontera-en-materia-de-probatica-2109#_ftn5

- GONZÁLEZ-MENESES GARCÍA-VALDECASAS, M.: "La función notarial en el medio electrónico". Conferencia pronunciada el 27 de octubre de 2011 en la *Academia Matritense del Notariado*. URL: https://www.elnotario.es/images/pdf/2710201-MANUELGONZALEZMENESES.pdf
- HERNÁNDEZ RAMOS, E.: "Conflicto entre la tecnología blockchain y la normativa de protección de datos". *Economist&Jurist* (11/01/2021). URL: https://www.economistjurist.es/articulos-juridicos-destacados/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos-2/
- NISIMBLAT, NATTAN: "El manejo de la prueba electrónica en el proceso civil colombiano". Universidad de los Andes. Facultad de Derecho. Revista N.º 4 (2010). URL: file:///C:/Users/UPEGUI/Downloads/Dialnet-ElManejoDeLaPruebaElectronicaEnElProcesoCivilColom-7507234.pdf
- NUNO, PATRICIA: "¿Qué es el sellado de tiempo?". *Ivnosys* (27/01/2020). URL: https://www.ivnosys.com/es/que-es-sellado-de-tiempo/OLIVA LEÓN, R., VALERO BARCELÓ, S. (Coords.) y VVAA: *La prueba electrónica. Validez y eficacia procesal*. Juristas con futuro, 2016. URL: https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf
- PASTORINO, CECILIA: "Blockchain: qué es, cómo funciona y cómo se está usando en el mercado". *Welivesecurity* (08/09/2018). URL: https://www.economistjurist.es/articulos-juridicos-destacados/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos-2/
- PÉREZ PORTO, J. y MERINO, M.: "Definición de GIF", *Definición.DE* (Publicado: 2018. Actualizado: 2019). Disponible en: https://definicion.de/gif/
- PÉREZ PALACI, J. E.: *La prueba electrónica: Consideraciones*. Universitat Oberta de Catalunya, 2014. URL: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf
- PINTO PALACIOS, F. y PURIFICACIÓN PUJOL, C.: *La prueba electrónica en la era digital*. Wolters Kluwer, Madrid, 2017

- RICHARD CONZÁLEZ, M: «La cadena de custodia en el proceso penal español», *Diario LA LEY* (8/11/2013). URL: https://fdocuments.mx/document/wolters-kluwer-espana-sa-no-se-identifica-ley-especial-probatica-12pdf.html
- ROSALES, F.: "Diferencias entre un Notario y el tercero de confianza". *Notariofranciscorosales.com* (02/02/2015). URL: https://www.notariofranciscorosales.com/diferencias-entre-un-notario-y-el-tercero-de-confianza/
- ROSALES, F.: "Notarios digitales, servicios y terceros de confianza". *Notariofranciscorosales.com* (12/09/2016). URL: https://www.notariofranciscorosales.com/notarios-digitales-servicios-y-terceros-de-confianza/
- ROSALES, F.: "Un Notario hablando de firma electrónica". *Notariofranciscorosales.com* (29/06/2015) URL: https://www.notariofranciscorosales.com/un-notario-hablando-de-firma-electronica/
- SEVILLA CÁCERES, F.: "Valoración de la prueba por el Tribunal de apelación". *Mundo jurídico.info* (23/11/2020). URL: https://www.mundojuridico.info/valoracion-de-la-prueba-por-el-tribunal-de-apelacion/
- TESONE, R., FERRER, J. y CAÑABETE, J.: "La obtención de la prueba electrónica, su acceso al proceso civil y la garantía de derechos en materia penal". *Economist & Jurist* (01/09/2012). URL: https://www.economistjurist.es/articulos-juridicos-destacados/la-obtencion-de-la-prueba-electronica-su-acceso-al-proceso-civil-y-la-garantia-de-derechos-en-materia-penal/
- "¿Qué es la biometría?", *Kimaldi*. Disponible en: https://www.kimaldi.com/blog/biometria/que_es_la_biometria/
- "¿Qué es un email certificado?", *Digitel TS*. Disponible en: https://digitelts.es/que-es-un-email-certificado

- VAN DEN EYNE, A.: “Retos relacionados con la prueba electrónica (parte I)”. *Eynde* (30/11/2013). URL: https://eynde.es/es/retos-relacionados-con-la-prueba-electronica-parte-i/
- VVAA: *La prueba civil a debate judicial. Estudios prácticos sobre prueba civil I*. Directores: Joan Picó i Junoy, Xavier Abel Lluch y Berta Pellicer Ortiz. Wolters Kluwer, Madrid, 2018.
- J.M.S.: “WhatsApp: qué es el cifrado «end to end» y por qué es importante”, *ABC* (actualizado: 12/01/2017). URL: https://www.abc.es/tecnologia/consultorio/abci-whatsapp-whatsapp-cifrado-201604060948_noticia.html?ref=https:%2F%2Fwww.google.com%