La prueba electrónica: Consideraciones

Autor: José Enrique Pérez Palací

www.prolex.org

mailto:prolexenrique@hotmail.com

@prolexblanes

http://prolexabogados.wordpress.com/

RESUMEN:

El análisis de la prueba electrónica en nuestro ordenamiento debe de terne en cuenta que dicha fuente de prueba ha sido introducida a partir de la LEC 1/2000, aun cuando la misma ya venía siendo atendida y considerada por nuestra jurisprudencia, así para el caso del fax.

Uno de los problemas que nos encontramos es dilucidar el cómo accede al proceso ya sea penal o civil o bien de otras jurisdicciones, y ello no sólo por cuestiones de "logística", sino por razones procesales ya que en muchos casos los tribunales son reacios a que se aporten los soportes informáticos, y tienden más a que el propio contenido de la prueba electrónica se aporte mediante los medios de prueba tradicionales.

El objeto del presente trabajo es dar unas pautas al profesional del derecho para que sepa qué caminos puede usar para que la prueba electrónica acceda al proceso con plenas garantías, y gozando de la seguridad jurídico-procesal ante una impugnación de la adversa.

Índice

1 PRINCIPIOS DE ACCESO DE LA PRUEBA ELECTRÓNICA AL PROCESO

El objeto de la prueba es lo que se quiere probar y la fijación de los hechos constituye la premisa menor del silogismo judicial, en cuanto que la sentencia está formada por una premisa mayor que es la norma jurídica, y una premisa menor, los hechos, los cuales deben subsumirse en el supuesto de hecho de la norma, y una conclusión, de modo que si los hechos se subsumieran a la norma, se aplicaría la misma.

Estos hechos podemos hallarlos en soportes clásicos (papel) o en soportes nuevos, como es el caso de la llamada prueba electrónica.

1.1 Fuentes y medios de prueba

Debemos distinguir entre las fuentes y los medios de prueba, que son los medios que tienen acceso al proceso, mientras que las fuentes son los hechos, a saber, la realidad que se quiere probar a través de la actividad o del instrumento, que permite justificar los hechos aseverados, o los refutados; por tanto, los medios de prueba son aquéllos que se recogen en el Artículo 299 de la LEC, el cual los clasifica en tres grupos: los clásicos o tradicionales: el interrogatorio de las partes, los documentos públicos y privados, el dictamen de peritos, reconocimiento judicial y el interrogatorio de testigos (Artículo 299.1 LEC), los medios de prueba denominados modernos o actuales: audiovisuales, los instrumentos informáticos (Artículo 299.2 LEC) y los medios de prueba futuros, cerrando nuestro legislador con una cláusula abierta que incorpora todos aquellos medios probatorios desconocidos en la actualidad (Artículo 299.3 LEC).

Por consiguiente, las fuentes de prueba que englobamos en la denominación de prueba electrónica son: las imágenes, las palabras y los sonidos que son la realidad pasada y recogida o almacenada en los medios de prueba, a saber, los soportes o instrumentos [1] [2].

Estas nuevas fuentes de prueba que se engloban en el Artículo 299.2 de la LEC deben acceder al proceso a través de un medio concreto de prueba, aunque "*nótese*

[1] Ortoño Artés, Carmen; El avance tecnológico y los nuevos medios de prueba en la LEC; Régimen jurídico de Internet, año 2001, Editorial La Ley, págs. 489-512.

[2] Sentencia de la Audiencia Provincial de Barcelona, sección 13, de 2 de mayo de 2007: "*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").*"

además que esos medios o instrumentos no son sino la adaptación del clásico documento a los nuevos soportes multimedia, pero no alcanzan a dar cabida al fenómeno de la red, donde las clásicas coordenadas de espacio y tiempo se enmarcan en una nueva dimensión. En efecto, el sistema de Internet va más allá de ser un soporte documental representativo de una realidad fáctica, pues se concibe como un conjunto de miles de redes de ordenadores conectados entre sí que permite el acceso a una inmensa fuente de información práctica y perfectamente disponible. Internet permite comunicarse a millones de personas de todo el mundo, remitir y recibir correos electrónicos, ofrecer y utilizar programas, publicitarse, realizar operaciones de márqueting y transacciones comerciales. Toda esa información fáctica se produce de modo instantáneo y simultáneo en el tiempo, y se exhibe sin las coordenadas clásicas de espacio-tiempo.", por tanto, "Internet no debe ser considerado como un medio de prueba sino como una, novedosa, fuente de prueba, procediendo pues analizar a través de qué medios de prueba (interrogatorios, documentos, dictámenes o reconocimiento) puede llevarse al proceso lo sucedido dentro de la red (fuente de prueba)." [3]

La prueba llamada electrónica, como medio de prueba, se encuadra, por tanto, en el grupo del apartado segundo del Artículo 299 de la LEC; ahora bien, antes de pasar a definir el concepto de prueba electrónica debemos profundizar en las relaciones existentes entre prueba y verdad, entendiendo verdad no como lo realmente ocurrido, sino como verdad de los enunciados y alegaciones de los escritos procesales sobre los hechos (demanda, contestación, denuncia, querella, entre otros); enunciados que es, en definitiva, lo que queremos probar, siendo la relación entre la prueba y la verdad, la finalidad de la actividad probatoria [4]. Por tanto, la prueba electrónica como los restantes medios probatorios tienen una finalidad relacionar esa prueba con la verdad de los hechos, verdad que para el caso del derecho penal tenderá a buscarse como verdad material, mientras que para el caso de las restantes ramas del derecho, la verdad que se busca es la verdad jurídica o formal.

1.2 La prueba electrónica: Consideraciones preliminares

Nuestra Carta Magna recoge en su Artículo 24.2 el derecho a utilizar los medios de prueba pertinentes para nuestra defensa, para la defensa de aquello que afirmamos y que queremos probar en el marco del proceso judicial, por lo que tenemos derecho a proponer prueba, que sea practicada, y que sea valorada por el Tribunal, así como derecho a recurrir para el caso de que sea inadmitida; no sea practicada, si ha sido admitida, o no sea valorada, a pesar de haber sido practicada.

Por tanto, tenemos un derecho a probar nuestras afirmaciones con los medios probatorios admitidos en derecho, respetando las reglas procesales sobre la aportación, práctica y valoración; ahora bien, en este mundo en el que nos hallamos cada vez estamos más sujetos a las llamadas nuevas tecnologías (TIC) que se centran en tres áreas interrelacionadas: la informática, el video y la telecomunicación, y cuyo desarrollo afecta a más de un área, y suponen la introducción en el mundo del derecho de nuevas

[3] INTERNET Y PRUEBA CIVIL por Jaume Alonso-Cuevillas Sayrol, RJC – año 2001, págs., 1079 y ss.

[4] Ferrer Beltrán, Jordi y otros, Estudios sobre la prueba, Editorial Universidad Nacional Autónoma de México, año 2006, 1ª edición.

fuentes de prueba a través de nuevos soportes y signos distintos de la escritura plasmada en un documento de papel.

Dentro del derecho de las nuevas tecnologías y dentro de los medios probatorios hallamos la prueba electrónica, cuya definición debe partir de una remisión a la normativa sustantiva y procesal, y así:

El Artículo 26 del Código Penal recoge bajo el epígrafe Concepto de documento lo que considera nuestro legislador que es documento, y así: "*todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*."

En el apartado primero del Artículo 743 de la LECRIM bajo el epígrafe: Medios de registro de la sesión. Documento electrónico. el legislador recoge una definición de documento electrónico y así dice: "*El desarrollo de las sesiones del juicio oral se registrará en soporte apto para la grabación y reproducción del sonido y de la imagen*."

Mientras que el Artículo 299 de la LEC enumera bajo el epígrafe: Medios de prueba, los distintos medios probatorios admitidos en derecho, entre los cuales y en su apartado segundo "*los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase* [...]".

La RAE nos da una definición de "*soporte*" como el material en cuya superficie se registra información, pudiendo ser ese material: el papel, la cinta de video, un CD, un lápiz de memoria (*Pendrive*), una cinta magnética, un disco duro (*Hard Disk Drive*), entre otros; estos soportes son medios de almacenamiento de datos, es decir, "*el antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho*." (RAE), mientras que los datos obtenidos a partir de esos soportes serían la información que nos sirve para adquirir el convencimiento del hecho afirmado, pudiendo estar dicha información recogida bien en una página web, un correo electrónico, una base de datos, una hoja de cálculo, un documento Word, un documento multimedia, etc., información que puede transmitirse en el marco de unas coordenadas de espacio y tiempo distintas de las habitualmente usadas en el marco procesal, de modo que una expresión que lesione la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación (injuria) insertada en una página web puede ser visionada por multitud de individuos, transmitiendo de este modo la expresión más allá de los confines cercanos al autor de la injuria, y así Twitter conecta instantáneamente a personas de todo el mundo y cualquier usuario registrado puede enviar un Tweet, es decir, un mensaje de 140 caracteres o menos que es público de forma predeterminada, y que puede incluir otros contenidos como fotos, videos y enlaces a otros sitios web (política de privacidad de Twitter), con lo cual el espacio tiempo - espacio ya no es el físico.

1.3 El acceso al proceso de la prueba electrónica: análisis comparado con los medios de prueba clásicos o tradicionales

La prueba electrónica puede acceder al proceso a través de los medios de prueba que se recogen en el Artículo 299.1 de la LEC, de modo que debemos analizar la introducción de los hechos acceden al proceso a través de los medios y soportes

probatorios, estos soportes pueden ser los incluidos en el Artículo 299.1 de la LEC, pudiendo esos hechos y afirmaciones recogidos en una página web, un correo electrónico y otros soportes informáticos en relación con el interrogatorio de las partes, los documentos privados y públicos, dictamen de peritos, reconocimiento judicial e interrogatorio de testigos:

El contenido de esos soportes puede a su vez acceder al proceso mediante el interrogatorio de las partes y/o testigos, la aportación de un documento privado, y así, por ejemplo cuando la parte interrogada reconoce o no impugna un correo electrónico aportado como documento y remitido desde la dirección electrónica de la otra.

Una página web, un blog, un *WhatsApp*, un folio *Excel*, un correo electrónico, etc. no son más que un documento, pero con la particularidad de que el medio o soporte donde se halla no es el tradicional, sino el informático; ahora bien, su contenido puede acceder mediante el uso de los medios clásicos, aportando la prueba electrónica al proceso como documento imprimiendo la imagen de la pantalla, o el correo electrónico y aportándolo al proceso como documento privado, ya público o incluso como pericial, cabiendo, incluso, que accede el contenido de la prueba electrónica a través del interrogatorio de las partes, de los testigos o del reconocimiento judicial, y ello previa proposición y admisión en el momento procesal oportuno, que sería **en el proceso civil,** en la audiencia previa, para el caso del Juicio Ordinario; y en la vista de juicio, para el caso del Juicio Verbal; y **en el proceso penal**: en la denuncia, en la querella, en la fase de instrucción, como cuestión previa en la vista de juicio oral, para el caso del Procedimiento Abreviado; en escrito de petición de diligencias, como cuestión previa, para el caso del Juicio de Faltas.

Los medios electrónicos, Internet (páginas web, blog's, redes sociales, chat públicos y privados, foros, comentarios, etc.), nuevos medios de comunicación (SMS, Whasap, Line, Skype, Messenger) han revolucionado no sólo las relaciones sociales, sino el acceso de la información, y en cuanto al derecho procesal los medios e instrumentos de acceso de los hechos al proceso judicial, por lo que el abogado debe conocer y vencer las dificultades y reticencias del foro (procuradores, abogados, jueces y fiscales) y, sobretodo, el iter preprocesal para reforzar la fuente de prueba que se pretende llevar al proceso mediante los medios de prueba, y así el letrado debe aportar el medio donde se halla el hecho que se quiere probar (un pendrive), volcar el contenido en un medio de prueba "clásico" (documento privado), protocolizar el correo electrónico, o solicitar que el notario otorgue acta de presencia (documento público), y acompañar junto con el documento un dictamen pericial.

Analizaremos la relación de la prueba electrónica con los llamados medios de prueba clásicos que se enumeran en el Artículo 299.1 de la LEC, y cómo puede acceder al proceso a través de los mismos:

A.- Documento privado, accederá aportando la página web o el correo electrónico impreso e incorporarlo al proceso en soporte papel, en tal caso la eficacia probatoria dependerá de la actitud procesal de la adversa, siendo útil proponer la prueba pericial si la adversa impugna en la fase procesal pertinente la autenticidad del documento (Artículo 326.2 LEC), puesto que en caso contrario, tendrá plena eficacia probatoria, alcanzado al hecho, acto o estado de las cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los intervinientes (Artículo 319.1 LEC).

B.- Documento público, accederá aportando acta notarial de la prueba electrónica, bien:

i. protocolizando el medio de prueba impreso con anterioridad por el particular; en tal caso, el notario hace constar la identidad, el documento entregado y la fecha en que lo recibe, de modo que el notario solo dará fe de la fecha de protocolización, y de la identidad de la persona compareciente y de que se le ha hecho entrega por éste del documento protocolizado (Artículo 145 del Reglamento Notarial), pero no de que dicho documento se corresponde con el contenido de la página web, o del correo electrónico.

ii. Mediante el acta de presencia prevista en el Artículo 199 del RN en relación con el Artículo 200, 3ª del mismo cuerpo legal, en que le son exhibidos al notario documentos procediendo el mismo a describirlos en el acta "tal y como resulten de su percepción".

iii. Mediante el testimonio de exhibición prevista en el Artículo 251 del RN en que el notario efectúa "*la reproducción auténtica de los documentos originales que les son exhibidos a tal fin o dan fe de la coincidencia de los soportes gráficos que les son entregados con la realidad que observen. El testimonio por exhibición no implica el juicio del notario sobre la autenticidad o autoría del documento testimoniado. Si el original testimoniado fuese a su vez copia de otro documento, el testimonio tampoco implicará la concordancia entre ambos, salvo que el notario la haga constar expresamente*." (Artículo 251 RN).

iv. Mediante el acta de exhibición "*el Notario describirá o relacionará las circunstancias que las identifiquen, diferenciando lo que resulte de su percepción de lo que manifiesten peritos u otras personas presentes en el acto, y podrá completar la descripción mediante planos, diseños, certificaciones, fotografías o fotocopias que incorporará a la matriz* " (Artículo 207 RN).

v. Mediante el acta de presencia acreditando la realidad o verdad del hecho que motiva su autorización, y así el notario "*redactará el concepto general en uno o varios actos, según lo que presencie o perciba por sus propios sentidos, en los detalles que interesen al requirente, si bien no podrá extenderse a hechos cuya constancia requieran conocimientos periciale*s." (Artículo 199 RN).

vi. Mediante acta de protocolización que tiene las características del acta de presencia, pero con la particularidad de que " *texto hará relación al hecho de haber sido examinado por el Notario el documento que deba ser protocolado, a la declaración de la voluntad del requirente para la protocolización* [...]" (Artículo 211 RN).

vii. Mediante acta de referencia cuyos requisitos son los mismos señalados para el caso de las actas de presencia, si bien "*el texto será redactado por el Notario de la manera más apropiada a las declaraciones de los que en ellas intervengan*, [...]" (Artículo 208 RN).

C.- Dictamen pericial, por las características intrínsecas y extrínsecas de la prueba electrónica cabe necesitar de una pericial informática y ello para "*conocer el contenido o sentido de una prueba o para proceder a su más acertada valoración*, [...]" (Artículo 352 LEC), pericial que puede ser o bien un instrumento ante la impugnación de la autenticidad o integridad del documento aportado, como auxiliar de la prueba, o bien como dictamen autónomo.

D.- Reconocimiento judicial examinando el propio órgano judicial de modo directo el objeto de la prueba bien en la sede del tribunal bien en el lugar donde se halle el soporte electrónico en el que se encuentra la prueba electrónica (Artículo 353 LEC), pudiendo solicitar a la proposición de que el proponente para el reconocimiento sea asistido de persona técnica o práctica en la materia, así como que se acuerden las medidas necesarias para lograr la efectividad del reconocimiento (Artículo 354.1 LEC), entre las cuales la entrada en el lugar donde se encuentra el medio de prueba, debiendo estar - en tal caso al respeto - y garantía de los derechos fundamentales, entre los cuales, el derecho a la intimidad, Inviolabilidad del domicilio, secreto de las comunicaciones, secreto profesional, tutela judicial efectiva, que se recogen en los Artículos 18 y 24 de la CE.

Y a través del interrogatorio de las partes, admitiendo o no impugnando la adversa la documental privada aportada, o bien a través del interrogatorio de testigos, los cuales en su interrogatorio reconocen hechos, así valga como ejemplo, que la parte contraria es la usuaria de un ordenador, es la única que tiene acceso al ordenador desde donde se envió el correo electrónico, o se "cargo" la imagen, etc.

2 NORMATIVA APLICABLE

En el marco legislativo español la admisibilidad de la prueba electrónica en los tribunales está regulada a través de disposiciones generales aplicables a la prueba clásica o tradicional, sin que exista una normativa específica aplicable. Este vacío legislativo que domina genera una inseguridad jurídica a los profesionales del derecho, ante esta realidad jurídica resulta necesaria una breve referencia a la normativa internacional y a la comunitaria.

Ese marco regulador se compone de una serie de normas procesales civiles, penales, laborales que afectan a las distintas ramas del derecho, así como disposiciones particulares sobre comercio electrónico, firma electrónica, sin que en todo ese marco encontremos una regulación específica para la prueba electrónica.

2.1 Normativa internacional

La Asamblea General de la ONU adoptó *las Resoluciones 55/63 y 56/121* sobre el combate contra el mal uso de las nuevas tecnologías de la información, destacando la necesidad de garantizar que cada país miembro adapte sus leyes para eliminar el ciberespacio de la delincuencia, intercambiando la información entre los estados y cooperar y coordinar a fin de una buena investigación penal concreta contra el mal uso de las TIC.

También cabe destacar:

Las *Recomendaciones* dirigidas a los gobiernos y a las organizaciones internacionales acerca del valor jurídico de los registros de ordenador, aprobados en el año 1985 por la CNUDMI [5].

Convención de la ONU sobre la utilización de las comunicaciones electrónicas en los contratos internacionales (Nueva York, 2005) [6].

[5] http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1985Recommendation.html http://www.uncitral.org/pdf/spanish/publications/sales_publications/UNCITRAL-s.pdf (págs. 45 y 46)

2.2 Normativa comunitaria

En nuestro ámbito comunitario coexisten dos modelos en relación con los requisitos que deben reunir las pruebas para su admisibilidad, por un lado, los que siguen un criterio muy amplio y que se basan en la libre consideración del juez para admitir o no la prueba electrónica, y así Austria, Dinamarca, Suecia, y Finlandia; y otro grupo, que tiene un criterio más restrictivo y que se remiten a los requisitos exigidos a los medios de prueba clásicos o tradicionales.

2.2.1 Convenio Europeo de Derechos Humanos

En primer lugar, cabe señalar el Convenio Europeo de Derechos Humanos que en su Artículo 8.1 recoge el derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia, mientras que en su apartado segundo, restringe la intervención del Estado, salvo por causas de "*seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*."

Dicho CEDH fue ratificado por España el 4 de octubre de 1979, y publicado el Instrumento de ratificación en el BOE de 10 de octubre de 1979 [7].

El Tribunal Europeo de Derechos Humanos (TEDH) ante una violación de lo dispuesto en el Artículo 8. Examina, primero, si la actuación del Estado demandado ha supuesto injerencia en el derecho reconocido en el artículo 8.1 del Convenio y, sólo si se responde afirmativamente a esta cuestión, se entra a considerar si la injerencia puede considerarse admisible conforme a lo dispuesto en el artículo 8.2., por lo que cualquier violación del derecho a la intimidad, al secreto de las comunicaciones y al derecho de inviolabilidad del domicilio puede buscar "*amparo*" ante el TEDH a través de demanda [8], cuyas causa de inadmisión principal es el no agotamiento de las vías de recurso internas, si bien cabe la interposición de .

2.2.2 Directiva 1999/93/CE

La Directiva 1999/93/CE por la que se establece un marco comunitario y unitario para la firma electrónica y que en su Artículo 2, 1) define qué entiende por firma electrónica, diferenciando entre firma electrónica y avanzada, y así "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación.", mientras que firma electrónica avanzada debe cumplir los requisitos de vinculación con el firmante, que se permita la identificación del mismo, que haya sido creada usando medios que el firmante puede mantener bajo su exclusivo control , y que esté "vinculada a los datos, de modo que cualquier cambio ulterior de los mismos sea detectable".

La misma Directiva establece en su Artículo 5 los efectos jurídicos de la firma electrónica, debiendo procurar los Estados miembros que la firma electrónica sea admisible en los procedimientos judiciales y no se niegue su eficacia jurídica.

[6] http://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf
[7] http://www.boe.es/boe/dias/1979/10/10/pdfs/A23564-23570.pdf
[8] http://www.derechoshumanos.net/denunciar/manuales/admisibilidad-demandas-TEDH-2010.pdf

Asimismo, cabe reseñar el Programa sobre cooperación policial y judicial en materia penal (AGIS), cuyo objetivo es favorecer la cooperación policial y judicial en materia penal y en el ámbito europeo en relación con la lucha contra los delitos telemáticos [9].

2.2.3 Más normativa a considerar

Decisión marco 2005/222/JHA del 24 de febrero de 2005 relativa a los ataques de que son objeto los sistemas de información y que tiene por objeto luchar contra la delincuencia informática y promover la seguridad de la información, y que define en su Artículo 1, b) el concepto de dato informático como "toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función" [10].

Por otra parte, no hay que dejar de mencionar la Resolución AG-2008-RES-08 aprobada por la Asamblea General de la OIPC-INTERPOL, en su 77ª reunión, tenida lugar en San Petesburgo del 7 al 10 de octubre de 2008, en que aprueba definir e impartir una formación adecuada a las unidades policiales intervinientes, así como coordinar misiones de apoyo en materia de informática forense, elaborar normas internacionales que regulen la búsqueda, el decomiso y la investigación de pruebas electrónicas, y seguir explorando la cooperación en este ámbito [11].

2.3 Normativa española

A nivel nacional tenemos que destacar:

– la Ley 59/2003, de 19 de diciembre, de firma electrónica, que define en su Artículo 3.1 define que la firma electrónica es el conjunto de datos en forma electrónica, que pueden ser utilizados como medio de identificación del firmante, diferenciando entre firma electrónica avanzada y firma electrónica reconocida, considerando la primera como la que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, estando vinculada la misma al firmante y a los datos, habiendo sido creada mediante medios que sólo el firmante puede mantener bajo su exclusivo control; mientras que la firma electrónica avanzada reconocida se basa "en un certificada reconocido y generada mediante un dispositivo seguro de creación de firma", teniendo el mismo valor que la firma manuscrita.

Define, asimismo, el concepto de documento electrónico como el redactado en soporte electrónico que incorpora datos firmados electrónicamente (Artículo 3.4 Ley 59/2003), pudiendo ser soporte de documentos públicos y privados, los cuales tendrán la eficacia que les otorgue la legislación aplicable, remite por tanto, a la normativa procesal civil.

Por otra parte, en su Artículo 3.8 otorga al soporte en que se hallan los datos firmados electrónicamente la categoría de prueba documental, así como el proceso a seguir si fuera impugnada la autenticidad de la firma electrónica reconocida y de la avanzada, confiriendo a la primera una mayor protección al proceder a la comprobación de si el prestador del servicio cumple con la obligación de garantizar la

[9] http://ec.eropa.eu/home-affairs/funding/2004_2007/agis/docs/annual_prog_2006_projects_es.pdf
[10] http://eur-lex.europa.eu/legal-content/ES7ALL?uri=CELEX:32005F0222
[11] http://www.interpol.int/es/content/download/5297/44458/version/4/file/AGN77RES08ES.pdf

confidencialidad, la autenticidad, conservación e integridad de la información, así como, la identidad de los firmantes; mientras que, a la segunda se remite a cuanto dispuesto por el Artículo 326 de la LEC.

– 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 Artículo 3 señala cuáles son los datos necesarios para rastrear e identificar el origen y destino de una comunicación, así como determinar la fecha, hora y duración de una comunicación, datos necesarios en cuanto que son los que deben conservar los operadores que prestan servicios de comunicación electrónicas.

– La Ley 34/2002, de 11 de julio, de Sociedad de servicios de la información, que en su Artículo 24 se remite al Artículo 3 de la Ley de firma electrónica, admitiendo como prueba documental "el soporte electrónico en que conste un contrato celebrado por vía electrónica".

– La Ley 41/2007, de reforma del mercado inmobiliario que modifica el Artículo 318 de la LEC dándole una nueva redacción e incorporando la mención a "documento electrónico" en su Disposición Final Sexta.

Por otra parte, no hay que dejar de mencionar el articulado aplicable de la LEC relativo a la prueba y que se contiene en el Libro II, Capítulo V (arts. 281 a 386), si bien son los Artículos 382 a 384 los que recogen los "*nuevos medios*" de prueba, aplicando analógicamente lo dispuesto para los documentos privados, en cuanto su aportación, proposición, práctica, impugnación y valoración, y es que la LEC no menciona a la prueba electrónica ni al documento electrónico en todo su articulado, salvo en los Artículos 146 y 147, en cuanto al soporte de grabación de las actuaciones, y en 318, en cuanto al modo de producción de la prueba por documentos públicos, señalando que harán prueba plena del hecho ya sea presentados en soporte papel o documento electrónico, así como en el Artículo 326.3 señalando que "*la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica*."

En cuanto a los derechos fundamentales no hay que olvidar el contenido del Artículo 18.1 ("*derecho al honor, a la intimidad personal y familiar y a la propia imagen*"), el Artículo 18.2 ("*El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito*"), el Artículo 18.3 ("*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*"), así como el Artículo 24 (Derecho a la tutela judicial efectiva), y el Artículo 120 (sobre la motivación de las sentencias, y por analogía las resoluciones que acuerdan la entrada y registro, y la interceptación de las comunicaciones).

Todo este abanico legislativo y la falta de unicidad y claridad ha conllevado a distintas clasificaciones de lo que se considera como soportes electrónicos, debiéndose reformular, por parte del legislativo, el noción de documento, incorporando los avances tecnológicos, superando la concepción dogmática de documento como soporte papel, huyendo de la escritura manuscrita o mecanográfica, y más cuando en el día de hoy todos los documentos, incluidos los de soporte papel, pueden ser objeto de manipulación, por lo que no puede ser el soporte papel *condictio sine qua non*, para dejar de admitir lo que es uso común en el tráfico jurídico, y más cuando el legislador

recoge en el Artículo 26 del Código Penal como concepto de documento "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica."

Cabe mencionar y destacar el listado recogido en el artículo doctrinal de Manuel M. Gómez del Castillo y Gómez, *Aproximación a los nuevos medios de prueba en el proceso civil* publicado en la revista "Derecho y conocimiento" de la Facultad de derecho de la Universidad de Huelva en que tras señalar que es difícil hacer una enumeración cerrada de los nuevos medios de prueba "*por la vertiginosa celeridad o rapidez con que se producen, hoy, las modificaciones técnicas y científicas*", sí que cabe distinguir los siguientes grupos: Instrumentos de captación y reproducción del sonido, Instrumentos de captación y reproducción de la imagen, Instrumentos de captación y reproducción de la imagen y del sonido, Instrumentos telemáticos, Instrumentos informáticos, Instrumentos derivados de la utilización de aparatos de control o medición e Instrumentos derivados de la utilización de aparatos registradores [12], clasificación que nos puede dar una idea de las dimensiones del asunto.

3 RÉGIMEN JURÍDICO DE LA PRUEBA ELECTRÓNICA EN LA LEY DE ENJUICIAMIENTO CIVIL

En primer lugar, hay que tener en cuenta que la LEC es de aplicación supletoria en defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares (Artículo 4 LEC).

En segundo lugar, que si bien es en los Artículos 382 a 384 que la LEC ha establecido una regulación para los denominados medios de reproducción de la palabra, del sonido y de la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso, no nos permiten estos tres artículos, del 382 al 384 de la LEC, esclarecer los principales problemas que suscitan especialmente la obtención y acceso, cuando se hayan podido vulnerar derechos y libertades fundamentales.

Las pruebas electrónicas acostumbran a ser muy frágiles, dúctiles y se pueden variar con suma facilidad por lo que es preciso asegurar la prueba. Lo podemos conseguir en sede judicial, mediante la correspondiente solicitud al Juez o bien previamente al proceso mediante la fe pública del Notario protocolizando una página web, un programa y su código fuente, un determinado dispositivo, como ya ha sido referenciado en el punto 1.3, B, igualmente, acudiendo al informe pericial judicial que acredite que no ha existido ninguna manipulación del tal prueba.

Al hilo de tal consideración debemos de abordar el cómo obtenerlas, el cómo conservarlas, cuándo proponerlas, el cómo practicarlas, el cómo impugnarlas, el cómo verificar su autenticidad y cómo deben ser valoradas por el juzgador, y así:

[12] http://www.uhu.es/derechoyconocimiento/DyC01/A05.pdf

3.1 Obtención de la prueba electrónica.

Frente a las pruebas tradicionales en la prueba electrónica tiene las siguientes características:

- Intangibles: Las evidencias electrónicas se encuentran en formato electrónico, siendo reproducibles, de fácil copia, diluyéndose las posibilidades de distinguir los originales de las copias
- Volátiles: Las evidencias electrónicas son mudables, inconstantes, en definitiva, manipulables, es decir, pueden ser modificadas.
- Delebles o destruibles: Las evidencias electrónicas pueden ser borradas o incluso cabe la posibilidad de que los soportes en los que se almacenan sean destruidos.
- Parciales: Normalmente, aunque no siempre es así, las evidencias electrónicas se encuentran en soportes que están en poder de quien las presenta como argumento de las pretensiones alegadas.
- Intrusivas: En ocasiones la recogida de las evidencias electrónicas puede afectar los derechos y libertades fundamentales de las personas como, entre otros, el derecho a la intimidad, el secreto de las comunicaciones, la libertad sindical o la protección de datos de carácter persona.

Y como si se tratara de un cubito de hielo se puede modificar, borrar, sobrescribir, desaparecer y destruir el soporte en el que se halla, y todo ello con facilidad; ahora bien, lo cierto es que siempre dejara un rastro que puede ser analizado por el perito informático.

Por tanto, es fundamental evidenciar que la prueba aportada al proceso se corresponde en su identidad con el original, puesto que ello afecta al contenido de la impugnación, pudiéndose impugnar la exactitud y autenticidad de la prueba aportada al proceso por falta de correspondencia con el original, debido a ello la aportación de la prueba electrónica al proceso debe hacerse respetando unas garantías que están íntimamente asociadas a las herramientas forenses y a la utilización de protocolos que permiten garantizar que la evidencia que deviene en prueba goza de las garantías procesales para que sea admitida y valorada por el juzgador, y es que dada la ubicuidad de la evidencia digital es raro que el delito no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos; y así, guardado en el hardware (Cámaras, ordenadores portátiles o de sobremesa, Pendrive, CD, móviles, etc.) y transmitido por los sistemas de comunicación (telecomunicaciones, Internet) a través de SMS, *WhatsApp*, Blog's, redes sociales, páginas web, preferentemente, ya como imágenes, ya como texto, ya como archivo.

Por tanto, conocida la existencia de la evidencia, y que la misma es pertinente, necesaria y útil, y que está bajo formato digital cabe conocer y saber:

Si la misma está en el mundo virtual, o si se halla en un lugar físico, y tras ello, seguir y obtener sin violar los derechos fundamentales, lo que las haría inválidas a los efectos probatorios, y ello en cuanto que la investigación de un delito está encaminada a la obtención de las pruebas que fijen los hechos, por lo que la entrada en el proceso de los hechos debe ser bajo un escrupuloso respeto de los derechos fundamentales y de las normas y garantías procesales.

A) Artículos 18.1 y 18.3 de la CE: el derecho a la intimidad y a la propia imagen, y el secreto de las comunicaciones.

El concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores, de forma que "*rectamente entendido*", el Artículo 18.3 CE consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas.

Ahora bien, sea cual sea el ámbito objetivo del concepto de la comunicación, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia *erga omnes*) ajenos a la comunicación misma.

Por ello si bien doctrinalmente se cuestiona que la policía puede interferir en el contenido de las conversaciones mantenidas entre dos participes, porque uno de los interlocutores autorice dicho acceso, esto es la irrelevancia constitucional resultaría objetable cuando la conversación está siendo observada o escuchada por agentes estatales con finalidades específicas de persecución, aún cuando alguno de los interlocutores hubiera admitido la injerencia del Estado (SSTEDH. Caso Kostowski contra Francia de 24.2.90, caso Allan contra Reino Unido de 5.11.2002 (TEDH 2002, 64), caso M.M. contra Holanda de 8.4.2003 (JUR 2003, 244791)), al ser evidente que los agentes de policía obtienen las fuentes de prueba a partir de la observación de la interlocución entre particulares sometidos a una investigación penal, por lo que la autorización prestada por uno de los investigados/interlocutores -en situación de detención en las propias dependencias policiales- para la audición por los agentes de las conversaciones telefónicas, no puede servir como mecanismo para eludir el régimen de injerencia cuando es el Estado el que protagoniza finalísticamente el acto investigatario, y así considera nuestro más Alto Tribunal en la reciente Sentencia núm. 16/2014 de 30 enero (RJ 2014\939), y es que el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional [13].

Y es que el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas (Sentencia del TC N. 114/1984, de 29 de noviembre).

[13] Sentencia del Tribunal Supremo de 12 de marzo de 2012, Sala de lo Penal (RJ 2012/4889)

Sobre los interlocutores, sin embargo, no pesa el deber de secreto, sino, en todo caso, y en virtud del Artículo 18.1 de la Carta Magna, un posible "deber de reserva" que dependiendo del contenido mismo de lo comunicado.

Por todo ello cabe diferencias entre el derecho fundamental al secreto de las comunicaciones y el derecho, también, fundamental a la intimidad, puesto que el que en el marco de una conversación telefónica, por correo electrónico, *WhatsApp* pone el móvil en modo altavoz, o muestra el email o *WhatsApp* o SMS a otros, no está violando el secreto de las comunicaciones, sin perjuicio de que con ese actuar al transmitir el mensaje y ponerlo en conocimiento de terceros ajenos entrase en la esfera «íntima» del emisor, lo cual sí puede constituir una vulneración del derecho a la intimidad.

Los derechos a la intimidad personal y a la propia imagen garantizados por el Artículo 18.1 de la Constitución Española, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda substraído a intromisiones extrañas, destacando la necesaria protección frente al creciente desarrollo de los medios y procedimiento de captación, divulgación y difusión de la misma y de datos y circunstancias que pertenecen a la intimidad.

Pues bien, en este sentido puede sostenerse que los objetos reconducibles al ámbito de intimidad relevante deben delimitarse atendiendo fundamentalmente al hecho de que se trate o no de objetos en los que se pueda materializar una proyección de la intimidad del sujeto, por lo que la obtención de evidencias que afecten a la intimidad debe contar con la autorización judicial, debiendo la misma respetar unas claras exigencias de legalidad constitucional, cuya concurrencia es necesaria para la validez de la intromisión en la esfera de la privacidad de las personas. La decisión sobre la restricción de este derecho, se deja, por tanto, en manos exclusivamente del poder judicial, de conformidad con el art. 18.3 CE concretamente, en el Juez de instrucción, a quien corresponde la ponderación de los intereses en juego, mediante un juicio acerca de la legitimidad, proporcionalidad y necesidad de la medida, el cual debe desprender de una resolución judicial motivada, adoptada en el ámbito de un proceso penal, y así, el Juez ha de atender necesariamente a varios aspectos:

EN PRIMER LUGAR, a la proporcionalidad, en el sentido de que ha de tratarse de la investigación de un delito grave. Para salvar la gravedad no solo se debe atender a la previsión legal de una pena privativa de libertad grave, sino además debe valorarse la trascendencia social del delito que se trata de investigar.

EN SEGUNDO LUGAR, a la especialidad, en tanto que la intervención debe estar relacionada con la investigación de un delito concreto, sin que sean lícitas las observaciones encaminadas a una prospección sobre la conducta de una persona en general.

EN TERCER LUGAR, a la necesidad, excepcionalidad e idoneidad de la medida, ya que solo debe acordarse cuando, desde una perspectiva razonable, no estén a disposición de la investigación, en atención a sus características y circunstancias, otras medidas menos gravosas para los derechos fundamentales del investigado e igualmente útiles para la investigación.

B) Artículo 18.2 CE: Inviolabilidad del domicilio

A efectos de domicilio, primero, debemos distinguir la afección e incidencia del derecho fundamental a la inviolabilidad del domicilio según la entrada y registro sea en un domicilio particular o en un domicilio social, y así:

El domicilio es un "*espacio apto para desarrollar vida privada" (STC 94/99 de 21.5), un aspecto que "entraña una estrecha vinculación con su ámbito de intimidad*", "el reducto último de su intimidad personal y familiar", especialmente clarificadora es la STS 1448/2005 de 18.11 (RJ 2005, 10063), que define de modo amplio el concepto de domicilio como "*cualquier lugar cerrado en el que pueda transcurrir la vida privada, individual o familiar*", o lo que es lo mismo, que "*sirva de habitación o morada a quien en él vive*", estimándose que constituye domicilio o morada, cualquier lugar, cualquiera que sea su condición y característica, donde vive esa persona o una familia, sea propiamente domicilio o simplemente residencia, estable o transitoria, incluidas las chabolas, tiendas de campaña, roulotes, etc., comprendidas las habitaciones de un hotel en las que se viva, por lo que cualquier entrada en el mismo requiere de autorización judicial,.

Ahora bien, este concepto amplio de domicilio que permite superar el concepto civil o administrativo, no autoriza, sin embargo, a incluir en él otros lugares, cuyo acceso depende también de la autorización del titular, en cuanto puede excluir la presencia de terceros en ellos, pero que por sus propias características no permiten afirmar que sean adecuados para que sus titulares desarrollen en ellos áreas o esferas de privacidad, es el caso del domicilio social de una entidad mercantil, de modo que la entrada y registro si es en una nave o almacén no tiene que someterse a las prevenciones del Artículo 569 LECRIM, ya que no constituye aquél domicilio alguno (SSTS 6.10.94 [RJ 1994, 7637] y 11.11.93 [RJ 1993, 8662]): por lo tanto, una nave, oficina o local comercial carecen de la protección que otorgan los apartados 1 y 2 del art. 18 CE, al no constituir, de modo evidente, un espacio de privacidad necesario para el libre desarrollo de la personalidad, de ahí que no puedan considerárseles incluidos dentro del ámbito de protección de la inviolabilidad del domicilio (SSTS 27.7.2001 [RJ 2001, 8118], 3.10.95 [RJ 1995, 7589], 27.10.93 [RJ 1993, 7872]), siendo particularmente explícita la STS 8.7.94 (RJ 1994, 6260), al afirmar que ni toda entrada y registro en un lugar cerrado exige la autorización judicial, ni los locales comerciales o almacenes que no constituyen morada de una persona gozan de la tutela constitucional del art. 18.2, sin que requieran, en consecuencia, para la entrada y registro en ellas de las mismas formalidades procesales que se imponen a los registros domiciliarios.

En relación con la obtención de prueba ilícita cabe mencionar la consolidada doctrina del vínculo o enlace de antijuridicidad, la llamada doctrina del fruto del árbol envenenado, la cual admite una corrección a través de otra teoría, del descubrimiento inevitable, es decir, si las circunstancias hubieran llevado necesariamente al mismo resultado, no es posible vincular causalmente la segunda prueba a la anterior, pues en tales casos faltara la conexión de antijuridicidad, que, en realidad presupone, en todos los casos, una conexión causal. Por lo tanto, allí donde la prueba se hubiera obtenido de todos modos, sin necesidad de recurrir a otra anterior, faltará la conexión de antijuridicidad, es decir, la relación causal de la primera con la segunda, y por consiguiente, la segunda prueba será lícita.

Ya la propia Fiscalía General del Estado en su Consulta 1/1999, de 22 de enero (RCL 2000, 878), sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones declaraba que "*la inmunidad constitucional no sólo previene la interceptación o captación en tiempo real sino cualquier forma de conocimiento antijurídico del contenido del mensaje o de las circunstancias significativas de la comunicación, aunque se produzca fuera del contexto temporal de la conexión*". Por tanto, el correo electrónico debe integrarse no tanto por las garantías de la intervención de la correspondencia cuanto por las garantías de la intervención telefónica, por lo que la intervención de correo electrónico exige que la resolución judicial especifique las concretas cuentas de correo electrónico afectadas, no siendo una buena práctica la de reseñar la línea telefónica habitualmente utilizada por el sujeto pasivo de la medida, ya que el mismo puede acceder a su cuenta o cuentas de correo electrónico a través de otras líneas.

Por tanto, no surtirán efecto, aquellas pruebas cuyo contenido derive directamente de la violación constitucional; por ejemplo, en el caso de que se declare la infracción del derecho al secreto de las comunicaciones, directamente no es valorable el contenido de tales escuchas, a saber, las propias conversaciones que se hayan captado mediante algún procedimiento de interceptación anticonstitucional, y en el supuesto de que lo conculcado sea la inviolabilidad del domicilio, no podrá ser valorado el hallazgo mismo obtenido.

Una vez obtenida la prueba debe aportarse y entrar en el proceso

3.2 Aportación de la prueba electrónica al proceso.

Hay que distinguir entre el modo en que la prueba electrónica se aporta o tiene su entrada en el proceso civil y el proceso penal, y ello en cuanto las características mismas de dichos procedimientos, y así:

1. Proceso civil

Es muy probable que no pueda aportarse directamente y por cuestiones logísticas e instrumentales, el hardware, es decir, el medio de prueba que recoge la fuente de prueba, por lo que habrá que trasladar la prueba electrónica al proceso en un soporte idóneo y adecuado, siguiendo un protocolo de actuación, y si es posible imprimirlo para presentarlo como un documento de referencia, indicando el archivo auténtico y original con el que puede ser cotejado (Artículo 265.2 LEC), facilitando de ese modo la accesibilidad del Juez [14].

Cabe también seguir el procedimiento señalado en el punto 1.3, B

2. Proceso penal

La Ley de Enjuiciamiento Criminal regula en su Título VIII (Artículos 545-588) los requisitos de la entrada y registro en lugar cerrado, la ocupación de libros y papeles y de la detención y apertura de la correspondencia escrita y telegráfica. Si conectamos dicho título con el contenido del artículo 18 de la Constitución, se pueden comprender las garantías exigidas para la diligencia de entrada y registro. Es necesario un auto de la autoridad judicial que esté conociendo o investigando un hecho con caracteres

[14] García Paredes, Artículo La prueba en juicio: ¿y si es electrónica? Revista de Contratación electrónica. N. 62, julio 2005

delictivos. Para garantizar la autenticidad del resultado de la diligencia se exigen una serie de garantías que se desarrollan a lo largo de los preceptos citados.

Para la obtención de la prueba electrónica debemos, por tanto, estar al respeto de los derechos fundamentales, por lo que si queremos como acusación que el imputado aporte la prueba electrónica que obra en su poder debemos solicitar al Juez instructor la entrada y registro en el domicilio, pudiendo éste "*decretar la entrada y registro de día o de noche, en todos los edificios y lugares públicos, sea cualquiera el territorio en que radiquen, cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación*." (Artículo 546 LECRIM), de tal modo que "*el auto de entrada y registro en el domicilio de un particular será siempre fundado, y el Juez expresará en él concretamente el edificio o lugar cerrado en que haya de verificarse, si tendrá lugar tan sólo de día y la Autoridad o funcionario que los haya de practicar*" (Artículo 558 LECRIM), y desde el momento en que acuerde la entrada y registro deben adoptarse las medidas de vigilancia convenientes para evitar la sustracción de los instrumentos, efectos del delito, libros, papeles o cualesquiera otras cosas que hayan de ser objeto del registro (Artículo 567 LECRIM).

La diligencia de entrada y registro se desarrollara según lo dispuesto por el Artículo 569 de la LECRIM, a saber, en presencia de Secretario Judicial, el cual levantara acta del resultado, de la diligencia y de las incidencias y será firmada por todos los asistentes, recogiéndose los "*instrumentos y efectos del delito y también los libros, papeles o cualesquiera otras cosas que se hubiesen encontrado, si esto fuere necesario para el resultado del sumario*", debiendo, exhibir "los objetos y papeles que se sospeche puedan tener relación con la causa", (Artículos 569, 572, 574 y 575).

Por otro lado, el Juez instructor puede, asimismo, acordar "*la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen*" (Artículo 579); como es de ver para el caso de la prueba electrónica debe aplicarse el precepto analógicamente relacionándolo con lo dispuesto en el Artículo 299.2 de la LEC.

Antes de realizar un entrada y registro en el domicilio para la incautación de los equipos Informáticos o Electrónicos debemos tener una metodología, y si bien no existen estándares establecidos con respecto a la Informática Forense hay muchas organizaciones trabajan en esto. El RFC 3227 se consolidó como guía para tratar la Evidencia Digital y la IOCE (International Organization of Computer Evidence), aunque actualmente se sigue la norma ISO 27037 [15] que está claramente orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia.

Los principios básicos en los que se basa la norma ISO 27037 son:

a) Aplicación de Métodos

La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.

[15] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

b) Proceso Auditable

Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados.

c) Proceso Reproducible

Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

d) Proceso Defendible

Las herramientas utilizadas deben de ser mencionadas y éstas deben de haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.

Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias:

e) La identificación

Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.

f) La recolección y/o adquisición

Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.

g) La conservación/preservación

La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la Cadena de Custodia, la integridad y la originalidad de la prueba.

Y es que las orientaciones de la Norma ISO 27037:2012 están encaminadas a la "*obtención de información y evidencias de los bits que se encuentran en los dispositivos*

físicos de almacenamiento o virtuales en las redes que intervienen en la interacción de las personas con los sistemas" [16], lo cual requiere un contexto general de actuación que permita asegurar que los procedimientos aplicados en la pericia son adecuados y con arreglo a normativa legal.

La orientación de la norma ISO 27037:2012 va dirigida a los siguientes dispositivos, sin que ello no implique su no aplicación analógica para los restantes dispositivos o soportes informáticos:

– Medios de almacenamiento digitales utilizados en ordenadores tales como discos duros, discos flexibles, discos ópticos y magneto ópticos, dispositivos de datos con funciones similares

– Teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria

– Sistemas de navegación móvil

– Cámaras digitales y de video (incluyendo CCTV)

– Ordenadores de uso generalizado conectados a redes

– Redes basadas en protocolos TCP / IP y otros.

– Dispositivos con funciones similares a las anteriores

4 CASUÍSTICA: JURISPRUDENCIA

4.1 WhatsApp, prueba válida:

– Auto del Tribunal Supremo de 14 de febrero de 2013 que considera este sistema de mensajería instantánea como un medio válido para acreditar determinados hechos.

En dicho asunto, el condenado por un delito contra la salud pública por tráfico de sustancias estupefacientes, decidió recurrir ante el Tribunal Supremo la sentencia de la Audiencia Provincial de Madrid que lo había condenado, siendo la base de su recurso la vulneración del artículo 18.3 de la CE , en relación con el artículo 24.2 de la misma (derecho a la presunción de inocencia) dado que éste interpretaba que las conversaciones intervenidas en el teléfono del recurrente por medio de la aplicación whatsapp de su teléfono, eran nulas por vulnerar la doctrina jurisprudencial sobre las escuchas telefónicas, el hallazgo casual y el descubrimiento inevitable.

El Tribunal Supremo (partiendo de la doctrina del Tribunal Constitucional que posibilita el que por resolución judicial se pueda acordar la medida de intervención telefónica siempre que se expresen o exterioricen las razones fácticas y jurídicas que apoyan la necesidad de tal intervención) entendió que el acceso por parte de los agentes de la Guardia Civil al contenido de las aplicaciones del teléfono móvil del condenado, si bien afectaba al derecho constitucional al secreto de las comunicaciones protegido en el artículo 18.3 de la CE, se llevó a cabo previa autorización judicial mediante auto adoptado como consecuencia del requerimiento de la Policía Judicial para el encendido del teléfono y la comprobación de los datos obrantes en el mismo.

[16] LOPEZ RIVERA, R. (2012) Peritaje informático y tecnológico. Un enfoque teórico-práctico: ISBN 978-84-6160-895-9

En dicho auto judicial se autorizaba al equipo de Policía Judicial para que pudiera encender el terminal telefónico intervenido al recurrente, al objeto de comprobar y reseñar datos sobre las comunicaciones existentes vía SMS, vía MMS, vía Whatsapp, y datos de contacto de la agenda... Partiendo de esa base, no puede alegarse que se haya vulnerado el derecho al secreto de las comunicaciones.

– Sentencia de la Audiencia Provincial de Cádiz, 31/2014 de 28 enero. JUR 2014\95996 "[…] *pues no habiendo declarado los dos implicados, de la existencia de lesiones no puede desprenderse el origen de su autoría y unos mensajes de wasap sobre los que ningún técnico ha declarado y que no consta que sean veraces o emitidos por el apelante o que no hayan podido ser manipulados, no es suficiente prueba para sustentar en ella el pronunciamiento condenatorio que se combate, razón que hace procedente la estimación del recurso* […]".

– Sentencia de la Audiencia Provincial de Pontevedra, 10/2014 de 10 enero. JUR 2014\25448 "[…] *la prueba que sustenta la condena del recurrente, aparte del dato objetivo de la existencia de los carteles y whatsapp, de indiscutible carácter vejatorio y ofensivo, se deriva de las manifestaciones de la denunciante, pues no consta siquiera la titularidad del teléfono desde el que se envían los mensajes y las declaraciones de los testigos no son concluyentes. Tales datos, se estima son manifiestamente insuficientes para deducir de ellos, con el nivel de certeza necesario para sustentar una Sentencia condenatoria* […]".

– Sentencia de la Audiencia Provincial de Madrid, 12/2013 de 5 abril. JUR 2013\175198 "*Mensajes, enviados a través del whatsapp, que han resultado transcritos en el Juzgado de Violencia Sobre la Mujer nº 3 de Madrid, al inicio de las actuaciones judiciales que, como ya anticipábamos adquieren un singular valor probatorio, porque, tanto por la secuencia horaria en que las comunicaciones entre Celia y Concepción se realizan, como por el contenido de las mismas, suponen un elemento de corroboración objetiva puntual y exacta de lo declarado, coincidentemente, por las dos testigos*."

– Sentencia de la Audiencia Provincial de Madrid, 1260/2012 de 1 octubre. JUR 2012\341849 "*También considera que el contenido las WHAT'S APP son fácilmente manipulables, y se pueden borrar parte las conversaciones, por lo que entiende que el libre acceso que han tenido los agentes a estas WHAT'S APP, contactos y todo tipo de aplicaciones del teléfono móvil del terminal de don Elias vulneran el artículo 18,3 de la Constitución y por lo tanto considera que debe existir una nulidad de todas las transcripciones y los las pantallazos incorporados a las actuaciones* […].