VISTO BUENO DEL O DE LA TUTOR/A DEL TRABAJO FIN DE MÁSTER

El/La Profesor/a Ana T. Afonso Barrera, como Tutor/a del Trabajo Fin de Máster titulado "La prueba electróncia en el proceso penal", realizado por ……Dª SILVIA AFONSO DORTA, informa favorablemente el mismo, dado que reúne las condiciones necesarias para su defensa.

En cumplimiento de lo previsto en la Guía docente de la asignatura, se propone la calificación de …7.5……., en atención a la profundidad del tema tratado, sistemática utilizada y consultas jurisprudenciales y bibliográficas realizadas.

En La Laguna, a 12 de marzo de . 2021.

Fdo.: Ana T. Afonso Barrera..

C/ Padre Herrera s/n
38207 La Laguna
Santa Cruz de Tenerife. España

T: 900 43 25 26

ull.es

LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL

Electronic evidence in criminal proceeding

Alumna: Doña Silvia Afonso Dorta.

Tutora: Doña Ana Teresa Afonso Barrera.

Máster de Acceso a la Abogacía.

2020/2021

ÍNDICE

I.- INTRODUCCIÓN……..……..4

II.- CONCEPTO…….……..5

III.- CLASES DE PRUEBAS ELECTRÓNICAS…….……6

3-1.- El documento electrónico……..……..6

3.2.- El correo electrónico……...8

3.3.- SMS…….……8

3.4.- Páginas webs……..……..9

3.5.- Grabaciones de sonido……..……..9

3.6.- Fotografía digital……..……..10

3.7.- Videograbaciones……..……..11

3.8.- Redes Sociales……....12

3.9.- Whatsapp y aplicaciones de mensajería instantánea similares……14

IV.- ASPECTOS PROCESALES DE LA PRUEBA ELECTRÓNICA……15

4.1.- Diligencias de investigación……..15

4.2.- El acceso de las partes a la investigación de la prueba electrónica……..18

4.3.- La pericial informática en el proceso penal……19

V.- PROBLEMAS JURÍDICOS DERIVADOS DEL USO DE LA PRUEBA ELECTRÓNICA……22

5.1.- Posible afección de los derechos fundamentales…….22

5.2.- Teoría del *"fruto del árbol envenenado"* con especial aplicación a la prueba electrónica……...24

5.3.- La alteración y fragilidad de la prueba electrónica……..25

5.3.1.- Medidas para conservar la prueba electrónica…….26

VI.- CONCLUSIONES…….29

VII.- BIBLIOGRAFÍA……..31

ABSTRACT

This research work analyzes the current conception of electronic evidence in criminal proceedings, the kinds of evidence that the parties can use, the investigation procedures to obtain them during a judicial or police investigation, the advantages and drawbacks that it has, and how to overcome these drawbacks to guarantee the integrity of the technical evidence provided by the computer science by ensuring that it lasts until the moment of its evaluation in the criminal process.

RESUMEN

En este trabajo de investigación se analiza la concepción actual de la prueba electrónica en el proceso penal, las clases de pruebas que pueden utilizar las partes, las diligencias de investigación para obtener las mismas en el trascurso de una investigación judicial o policial, las ventajas e inconvenientes que tiene la misma, y como superar estos inconvenientes garantizar la integridad de la prueba mediante técnicas que nos aporta la informática para que perduren hasta el momento de su valoración en el proceso penal.

I.- INTRODUCCIÓN

6 horas y 54 minutos es la media que pasan los españoles al día en Internet o haciendo uso de algún dispositivo electrónico[1]. Estos dispositivos se han convertido en la prolongación artificial de nuestra comunicación, nuestra memoria, y guardan todos los datos personales y movimientos.

Esto ha significado un cambio en nuestra vida facilitando la forma de concebir las relaciones con los demás, la interacción con el entorno y la creación de negocios jurídicos pero, paralelamente a estos cambios positivos, las nuevas tecnologías han contribuido a modernizar la delincuencia y a un crecimiento mayor de la misma. No es hasta la reforma de 2015 cuando el Código Penal[2] comienza a incluir en su texto la tipificación de delitos cometidos por medio de la tecnología, delitos que podríamos calificar como "*delitos informáticos*"[3] y, a consecuencia de ello hoy en día son frecuentes las pruebas que las partes personadas en un proceso penal presentan ante el Tribunal para acreditar las afirmaciones que defienden y que se encuentren recogidas en un dispositivo o formato digital, e incluso se utilizan estas pruebas en procesos por delitos no calificados como informáticos.

El tema del que versa este trabajo se ha escogido atendiendo a la importancia y relevancia de la era digital en la que vivimos, y que constituyen en la realidad el hecho de que cada vez está más presente el uso de la tecnología que afecta a las cuestiones jurídicas, y en este caso que nos ocupa, a la prueba presentada por las partes personadas en el proceso penal que previamente se ha generado mediante el uso de un dispositivo electrónico. Se hará una valoración de las distintas pruebas que los abogados pueden hacer valer dentro del procedimiento, la dificultad y problemática que entraña en las diligencias de investigación, así como las posibles soluciones para preservar su integridad hasta el momento de la valoración.

[1] SIMON KEMP (2021), "Digital 2021: Global overview report", Datareportal.
[2] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 22 de noviembre, del Código Penal.
[3] HERNÁNDEZ DIAZ L, "El delito informático", Eguzkilore, País Vasco, 2009, p.230-232.

II.- CONCEPTO

Gimeno Sendra definía la prueba como aquella actividad que realizan las partes procesales encaminada a obtener el convencimiento y la certeza del Tribunal que decide en el litigio sobre aquellos hechos que dichas partes afirman[4].

La era digital nos ha traído, de una forma casi equiparable al fenómeno supralumínico, cambios en la forma de concebir esta prueba en el proceso penal, naciendo el nuevo concepto de la prueba electrónica, informática o digital, entendiéndose a priori como aquella información que encontrándose en soportes electrónicos sea capaz de acreditar hechos que pretendan probarse. La clave de esta prueba es que la información que tiene como fin la acreditación de estos hechos se encuentre recogida, o se pueda transmitir, por medios electrónicos que serán los que se incorporen al proceso[5].

Esta definición podría acercarse al concepto que se quiere desarrollar en este trabajo, sin embargo, hasta la fecha en nuestro ordenamiento jurídico no hay normativa, ni comunitaria ni propia, que defina exactamente lo que es la prueba electrónica, la Real Academia de la Lengua Española utiliza una terminología algo más técnica considera que la prueba electrónica se compone de un elemento hardware y un software, una parte física que conserva el documento y una parte intangible compuesto por interfaces informáticas. Y el artículo 3.5 de la Ley 59/2003 de 19 de diciembre[6], de firma electrónica, define el documento electrónico como *"la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"*.

El principal problema en este tema, es que no existe en nuestro derecho un procedimiento probatorio particular y especial que valore la prueba presentada por medios electrónicos para determinados procesos. Le serán aplicable por analogía las normas relativas a los medios probatorios recogidos en los artículos 299.2, 299.3 de la Ley de Enjuiciamiento Civil, (en adelante LEC*)* y el artículo 11.1 de la Ley Orgánica del Poder Judicial, (en adelante LOPJ), los medios de reproducción propios de la imagen, la palabra y el sonido, o aquellos que resulten necesarios en cada caso, las

[4] GIMENO SENDRA, J V, Derecho Procesal Penal, Ed: Aranzadi, Madrid, 2020, p 371.
[5] DELGADO MARTÍN J, La prueba electrónica en el proceso penal, Diario La Ley, número 8.167, 2013 p I.
[6] La mencionada Ley se encuentra actualmente derogada, la cual ha sido sustituida por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

recogidas en los artículos 382.1 y punto 2.2 de la LEC que permite a las partes reproducir ante el tribunal estas imágenes, palabras y sonidos mediante instrumentos que graben y filmen los mismos, admitiendo cualquier soporte multimedia, así como aquellos dictámenes que validen la autenticidad de lo presentado. Tampoco existe un modo especifico de preservar y conservar la prueba electrónica para mantener su cadena de custodia, garantizando con ello su autenticidad en el momento probatorio del proceso.

III.- CLASES DE PRUEBAS ELECTRÓNICAS

Pinto y Pujol extraen un listado de las pruebas electrónicas que más se aportan en el proceso judicial, clasificándolas en[7]:

3.1.- EL DOCUMENTO ELECTRÓNICO

Tal y como se ha intentado explicar anteriormente, una primera aproximación al concepto de documento electrónico puede definirse como una manifestación de voluntad o una representación de un hecho de interés parar el proceso que puede obtenerse a través de un medio reproductivo como la fotografía, las cintas de vídeo, los discos de ordenador, una factura electrónica, entre otros.

Las tres ideas principales sobre el documento electrónico son las siguientes[8]:

La primera, concibe como documento electrónico aquel documento en el que la informática ha contribuido a su elaboración, por lo que se incluyen tanto las pruebas como un e-mail, video, fax o similares, como cualquiera generada por un medio de reproducción de archivos, o aquellas contenidas en instrumentos informáticos, como bases de datos, pendrives etc.

[7] PINTO PALACIOS F y PUJOL CAPILLA P, La prueba en la era digital, Ed. Wolters Kluwer, Madrid 2017, p 38-62.
[8] ABEL LLUCH X, La prueba electrónica, series estudios prácticos sobre los medios de prueba, ESADE 2010, p 27-29.

La segunda, para que un documento se considere electrónico en cualquiera de las fases de las cuales está compuesto, ha debido intervenir un equipo o herramienta informática.

Y la tercera y última, se define, como veíamos anteriormente, en el artículo 3.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica[9], este concepto podría ser quizá el más estricto y técnico dando una idea más correcta de la definición.

El documento electrónico está compuesto por una serie de elementos de entre los que podemos encontrar los siguientes:

- El s*oporte:* se trata del objeto que puede presentarse ante un procedimiento judicial para su examen, existen soportes de muchos tipos, disco duro, pen drive, y cualquier otro derivado.

- *El contenido:* La información contenida en el soporte del documento se encuentra grabada con un lenguaje binario, siendo necesaria un intercesor para ser entendida, de esto se encargan los medios informáticos que muestran el contenido, como programas softwares, o elementos auxiliares como dispositivos de reproducción, del tipo que sean.

- *El autor:* Demostrar la autoría de un documento electrónico, sería la parte más controvertida de hacer valer la prueba en un proceso judicial, pues, tal y como afirma el autor, en muchas ocasiones, solo se puede acreditar que el archivo ha sido creado en un determinado ordenador, pero no la autoría de esta, siendo para ello importante darle un mayor peso a la firma electrónica, ya que esta firma aporta al documento certificando de esa forma la autoría.

- *Fecha:* En un documento electrónico se asigna de forma automática por el programa informático que lo haya creado, no obstante, hay que tener en cuenta lo que sostiene el autor al señalar que la fecha puede ser modificada por muchos programas, por tanto, una manera de verificar la fecha puede ser a través, nuevamente de la firma electrónica o manuscrita, en el caso de haberse consignado la misma.

[9] Esta normativa se encuentra hoy en día derogada.

3.2.- CORREO ELECTRÓNICO

Como afirma la doctora Vera Delfa[10], el correo electrónico puede definirse como el sistema de mensajería que permite intercambiar textos digitalizados, considerándolo el más antiguo de la era de Internet. Estos mensajes se almacenan en un servidor mediante un buzón identificado con una dirección electrónica concreta, y con la que se accede a través de contraseña privada.

Una forma de asegurar la eficacia probatoria del correo electrónico es solicitar acta notarial, en la que se dé fe sobre sobre el contenido de los e-mails o correos electrónicos que se encuentran en un servidor, las direcciones de los usuarios que han intervenido en la emisión y recepción de ese contenido, así como las fechas en las que se han hecho este intercambio de información. De igual forma, aportado acuse de recibo donde se haga constar la recepción de ese mensaje al destinatario.

Es importante tener en cuenta, que la aportación de correos electrónicos al proceso, normalmente se realiza mediante formato papel, aunque de acuerdo con el articulo 384 LEC, pueden ser aportados mediante otros instrumentos propuestos por las partes. Al respecto, Abel Lluch[11] sostiene que estas pruebas, pueden acceder al proceso a través de la prueba documental, y se trata de fuentes de prueba que se sirven de un soporte informático (internet) o electrónico (documento electrónico), sin necesidad de su traslación a un soporte papel para que puedan desplegar eficacia probatoria, pero siendo bastante complicado que esta aportación se haga en la práctica.

3.3.- SMS (*"Short Message Service"* o Servicio de Mensajes Cortos)

Se trata de un servicio de mensajería telefónica que permite enviar mensajes de texto de corta extensión. Estos mensajes se envían desde un número de teléfono a otro pasando por un servidor, que se encarga de reenviarlo al destinatario. Si este dispositivo móvil fuera intervenido en una investigación judicial se podrá acceder al contenido de estos mensajes mediante este servidor, una diferencia con las más modernas aplicaciones de mensajería instantánea, no alojan ningún servidor sino en los propios

[10] VERA DELFA C, El correo electrónico: el nacimiento de un nuevo género, Tesis Doctoral, Facultad de Filología, Universidad Complutense de Madrid, Madrid, 2006.
[11] ABEL LLUCH X, La prueba documental, series estudios prácticos sobre los medios de prueba, Op. Cit, p 30.

teléfonos de los usuarios, contando con sistemas de encriptado mucho más sofisticados, pero que no impiden que se pueda llegar al contenido.

3.4.- PÁGINAS WEBS

Se define como un conjunto de informaciones de un sitio web que se visualizan en una pantalla, pudiendo incluir textos, contenidos audiovisuales y enlaces con otras páginas[12]

Continuando con Pinto y Pujol, a esta información se puede acceder por Internet previa identificación de un enlace en un navegador: Internet Explorer, Firefox o Google Chrome, entre los más conocidos.

Unos de los principales hándicaps que presentan las páginas web en cuanto a su eficacia probatoria, es la posibilidad de ser modificadas, de modo, que el contenido deje de existir para cuando se pretenda hacer valer la prueba en un proceso penal. Por tanto, una solución a este problema podría ser levantar un acta notarial en la que se dé fe de la existencia de dicha página web y de su contenido en un momento determinado. Otra de las soluciones que reflejan los autores es el reconocimiento judicial de la página web, esto es, la cibernavegación judicial, para que el Tribunal pueda comprobar por si mismo el contenido de la web.

Los autores señalan que también un medio para probar los hechos ocurridos en una web puede constatarse y reconocerse a través de esta cibernavegación judicial. De igual forma, se admite que el contenido de una página web se pueda reconocer mediante el interrogatorio de las partes o de testigos. Algo que sucedería con cualquier otro medio de prueba mencionado.

3.5- GRABACIONES DE SONIDO

Las grabaciones de sonido exigen, como sostiene Abel Lluch, unas mayores garantías para ser incorporado al proceso, entre las que destaca, *"el respeto de la intimidad, la puesta a disposición del Tribunal de los soportes que registran la conversación y verificación de la autenticidad para evitar posibles manipulaciones"*. Para evitar su manipulación, es conveniente realizar un *"cotejo de voces"* de forma que permita averiguar si el registro fonográfico corresponde a una determinada persona y

[12] Definición aportada por la RAE.

por otro lado, la aportación de un dictamen pericial donde se acredite que no se ha manipulado, así como los métodos de *"acústica forense"*, que se refiere a los medios de ingeniería acústica para averiguar la identidad de los participantes en un audio.

Una cuestión importante es que las grabaciones de sonido puedan ser incorporados al proceso si se dan los requisitos exigidos por la jurisprudencia desde la sentencia del Tribunal Constitucional, Sala Segunda, de 29 de noviembre, de forma que las grabaciones realizadas entre los participantes de una conversación pueden surtir efectos probatorios, no en cambio, cuando la grabación se utiliza con una finalidad distinta, como puede ser su venta o difusión, revelando con ello secretos.

3.6.- FOTOGRAFÍA DIGITAL

La fotografía digital no difiere de la fotografía convencional, la cual, una vez capturada se conserva en la memoria interna del dispositivo electrónico que la haya capturado. Como ya hemos mencionado antes, ésta puede incorporarse al proceso tanto en formato papel como en soporte digital cuando se haya almacenado en algún dispositivo electrónico de memoria.

Uno de los problemas que presenta la fotografía digital en la fase probatoria es la identificación de la fecha, y en algunos casos, el lugar donde ha sido tomada, problema que puede ser resuelto mediante la solicitud de un acta notarial de presencia, para que se persone en el lugar donde se ha tomado la fotografía y pueda constatarla, además, de determinar cómo se encuentra el lugar en una fecha determinada en comparación con la fotografía tomada. Asimismo, puede plantearse la posibilidad de tomar la fotografía mediante aplicaciones específicas que certifiquen dichas fotografías, como por ejemplo la plataforma *"SafeStamper"*, de certificación digital, entre muchas otras.

Por otro lado, hay que tener en cuenta que las fotografías digitales pueden ser manipuladas fácilmente hoy en día, en cuanto a los objetos que aparecen en ellas, los sujetos, etc. Por lo que siempre se podrá ir acompañado de un informe pericial para constatar que las mismas no han sido manipuladas.

3.7.- VIDEOGRABACIONES

Consiste en la captación y grabación de imágenes a través de un dispositivo electrónico (vídeocámara, teléfono móvil, entre otros). Es importante tener en cuenta que en función de quién realice esta grabación, estará condicionada a unos requisitos u otros. En este sentido, debemos diferenciar las videograbaciones, en este caso, de vigilancia, recogidas por las Fuerzas y Cuerpo de Seguridad en lugares públicos, regulado en la Ley Orgánica 4/1997, de 4 de agosto. Debemos destacar respecto a estas grabaciones, que la utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima, exigiendo la existencia de un razonable riesgo para la seguridad ciudadana, o de un peligro concreto (artículo 6 de la Ley). Resulta fundamental destacar lo sostenido en su apartado 5 para hacer valer las mismas como medio de prueba, al establecer que no se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de viviendas ni de sus vestíbulos salvo consentimiento del titular o autorización judicial, así como de otros lugares abiertos o cerrados cuando afecte de forma directa y grave a la intimidad de las personas, debiéndose destruir de forma inmediata las imágenes obtenidas sin estos requisitos. El artículo 7.1 del mentado texto legal reza que *"cuando la grabación captara hechos que pudieran ser constitutivos de delito, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos a disposición judicial con la mayor inmediatez posible, y en todo caso, en el plazo máximo de setenta y dos horas desde su grabación"*.

Por otro lado, pueden darse las videograbaciones efectuadas por seguridad privada, regulado en el artículo 42 de la Ley 5/2014, de 4 de abril. En su apartado 4 se establece que "*las grabaciones realizadas por los sistemas de videovigilancia de Seguridad Privada no podrán destinarse a un uso distinto del de su finalidad*." Cuando las mismas se encuentren relacionadas con hechos delictivos, se aportarán, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales. Añade el apartado 6, que *"en lo no previsto en la Ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad"*.

En tercer lugar, las videograbaciones tomadas por la Policía Judicial en el marco de un proceso penal, las cuales, deberán ajustarse al artículo 588. a) quinquies de la

LECRIM. En este sentido, "*se podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos*". Además, podrá afectar a personas diferentes del investigado siempre que se reduzca de forma relevante la utilidad de la vigilancia o existan indicios de la relación entre estos sujetos o hechos de los que verse la investigación.

Y por otro lado, hoy más extendido, debido al uso creciente de los smartphones o teléfonos pueden darse las grabaciones realizadas por particulares a través de cámaras ocultas. Los particulares, la antigua jurisprudencia del Tribunal Constitucional alegaba que no puede primar la prevalencia del derecho a la información sobre el derecho a la intimidad y a la propia imagen cuando el conocimiento de la noticia se haya obtenido mediante la utilización de cámara oculta, aun cuando la información hubiera sido de relevancia pública (STC 12/2012, de 30 de enero), sin embargo, la reciente jurisprudencia del mismo Tribunal (STC 167/2020 de 19 de mayo), que da plena validez a aportar imágenes relevantes en un procedimiento penal aquellas imágenes captadas por cámara oculta.

3.8.- LAS REDES SOCIALES

El uso de redes sociales supone hoy en día una serie de disyuntivas que pueden afectar, entre otras cosas, al trascurso de un procedimiento penal, el principal problema es que la facilidad por crear una cuenta sin necesidad de que el individuo se identifique por algún medio oficial potencia el anonimato, suponiendo un problema en muchas ocasiones para determinar la autoría de la persona que ha cometido algún ilícito por medio de estas herramientas. En nuestro ordenamiento existe muy poca normativa, siendo en algunos casos nula, en cuanto a muchos de los problemas que derivan del uso de redes sociales, o cualquier otro medio tecnológico moderno, es por ello por lo que, le ha tocado a la jurisprudencia crear una base doctrinal conforme a estos conflictos.

En el proceso penal existe una importante sentencia pionera del Tribunal Supremo[13], que incorporó por primera vez como prueba determinante la captura de pantalla de una conversación realizada a través de una red social de moda en el

[13] STC nº300/2015, sala de lo penal, de 19 de mayo de 2015.

momento, de una menor a otra donde esta confesaba una serie de relatos de abuso sexual que recibía.

Sobre esta prueba electrónica el Supremo determinaba como conclusiones que:

- *"La prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas, ante 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.*

- *Cuando las pruebas son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. La parte que haya impugnado esta captura de pantalla deberá valerse de un informe pericial que demuestre; el verdadero origen de la comunicación, la identidad de los interlocutores, y por último, el contenido en su integridad".*

Esta doctrina ha sido reiterada en numerosas sentencias a partir de ese momento, dándole las sucesivas sentencias un valor importante a la prueba pericial informática cuando se impugne la autenticidad de los mensajes, debiendo aportarse informe, salvo que el investigado reconozca el contenido de los mensajes, o existan modos de expresión de los que se pueda entender sin lugar a duda que ha participado el acusado.[14]

En cuanto a la forma en la que se debe realizar este dictamen[15], ha suscitado numerosas cuestiones.

El primer hándicap que nos encontramos es que la información que se desea obtener puede que se encuentre en servidores o dispositivos fuera del territorio nacional, que dificultan aún más su obtención. Que los investigados alegando la protección de ciertos

[14] STS nº754/2015 Sala de lo Penal, de 27 de noviembre de 2015.
[15] SAEZ-SANTURTÚN PRIETO M, "La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 mayo de 2015", Diario La Ley, 2015, nº 8.637.

derechos fundamentales no de consentimiento y esto requiera el auxilio y autorización judicial, algunas aplicaciones de mensajería instantánea, las más utilizadas por los usuarios hoy en día, no utilizan un servidor donde almacenan los datos sino un sistema de cifrado que permite solo leer esos datos desde el dispositivo, limitando que intervengan en su lectura personas ajenas al receptor y el emisor.

3.9.- WHATSAPP Y APLICACIÓNES DE MENSAJERÍA INSTANTÁNEA SIMILARES.

Se estima que hoy en día más de mil millones de personas son usuarios de Whastapp, una plataforma que permite enviar mensajes instantáneos y que facilita las comunicaciones e intercambio de datos e información con otras personas. Como se señaló anteriormente la diferencia entre estas aplicaciones y los antiguos SMS es que estas utilizan un cifrado *"end-to-end"*[16], es decir, para garantizar la confidencialidad y la seguridad del contenido se anula la existencia de un servidor la que se pueda acceder para rescatar estos datos, siendo por tanto imposible acceder a ellos si no se accede previamente al dispositivo de alguno de los interlocutores, pero no solo se encuentra protegida la interacción de estos usuarios sino también cada mensaje que se envía, esta mejora aunque ha sido positiva para los usuarios que se preocupan por su privacidad, ha supuesto un obstáculo para la investigación de muchos delitos cometidos por este medio, que dificultan al programa SITEL.[17] Lo que si es cierto es la cantidad de pruebas provenientes de este medio que hoy en día se presentan en los Tribunal demostrando con los llamados "pantallazos" una conversación concreta, la problemática de esto es la facilidad de modificar esta captura que al fin y al cabo pasa a ser como una fotografía digital, siendo necesario por ejemplo, un cotejo en notaria que certifique los mensajes, la identidad de los comunicadores por medio del teléfono, y demás datos que sean relevantes y mantengan la integridad de la prueba.

[16] DELGADO MARTÍN J, "La prueba del Whatsapp", Diario La Ley, nº 8605, Sección Tribuna, 15 de septiembre de 2015.

[17] Conocido como el Sistema Integrado de Interceptación de Telecomunicaciones, Sistema Integrado de Interceptación Legal de Telecomunicaciones y Sistema Integral de Interceptación de las Comunicaciones Electrónicas cuya titularidad ostenta el Ministerio del Interior, con base en la sede central de la Dirección General de la Guardia Civil.

IV.- ASPECTOS PROCESALES DE LA PRUEBA ELECTRÓNICA

4.1.- DILIGENCIAS DE INVESTIGACIÓN

Las diligencias de investigación que recoge el artículo 299 de la LECRIM son actuaciones destinadas a comprobar la posible perpetración de un delito, teniendo por objeto unos hechos concretos, consiguiendo con ello muchas de las pruebas que luego se presentaran en la fase de juicio oral, salvo que hablemos de pruebas anticipadas o preconstituida, se busca por tanto, si existe o no una base para seguir el curso del proceso y la presencia de un ilícito penal, y los actos de prueba están encaminados a facilitarle a las partes aquella fundamentación fáctica que contengan sus escritos tanto de acusación como de calificación permitiendo al tribunal que sentencia extender el conocimiento sobre ellos en la declaración de los hechos probados en la sentencia.

La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECRIM, para fortalecer las garantías procesales y la regulación de las medidas de investigación tecnológica, incorporó a su texto doctrina asentada por el Tribunal Constitucional que recoge los requisitos que deben tenerse en cuenta en esta investigación y obtención de la prueba y que la limitan de una forma u otra para preservar los derechos fundamentales recogidos en la Constitución.

El juez o Tribunal encargado del enjuiciamiento de ciertos delitos, en nuestro caso, podrá admitir o no aquellas prueba que las partes puedan considerar pertinentes para defender sus intereses y constatar los hechos que desean probar, valorando de forma razonada y libre aquellos, sin embargo, siempre cumpliendo lo que reza el artículo 311 de la LECRIM[18], *"si no las considera inútiles o perjudiciales"*, se podrán practicar las diligencias de investigación propuestas por las partes personadas en el proceso y el Ministerio Fiscal, esto respecto al juez que instruya el sumario.

Respecto a la prueba practicada tanto en el procedimiento ordinario, conforme a los artículos 658 y 659 LECRIM, como en el procedimiento abreviado recogido en el artículo 785.1 del mismo texto legal, hay que tener en cuenta dos condicionantes para la

[18] **Artículo 311 del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal** – *"El Juez que instruya el sumario practicará las diligencias que le propusieran el Ministerio Fiscal o cualquiera de las partes personadas si no las considera inútiles o perjudiciales".*

admisión de estas pruebas. El primero de ellos, como ya hemos podido ver en la mención de los artículos anteriores, es que se traten de pruebas útiles y eficaces. El segundo, un requisito que como veremos en profundidad posteriormente trae consigo una conflictividad mayor, es que se propongan de acuerdo con el cumplimiento de todas las formalidades legales.

Ello amparado por la doctrina jurisprudencial en Sentencias del Tribunal Supremo del 14 de septiembre de 2006, así como algunas Sentencias dictadas por el Tribunal Europeo de Derechos Humanos en 1989 y 1990, que vienen en definitiva a fijar como debe ponderarse el juicio sobre la admisión e inadmisión de la prueba propuesta, "en el sentido de concerniente o atinente a lo que en el procedimiento en concreto se trata, es decir, que "*venga a propósito" del objeto del enjuiciamiento, que guarde auténtica relación con él; necesario, pues de su práctica el Juzgador puede extraer información de la que es menester disponer para la decisión sobre algún aspecto esencial, debiendo ser, por tanto, no sólo pertinente sino también influyente en la decisión última del Tribunal; y posible, toda vez que al Juez no le puede ser exigible una diligencia que vaya más allá del razonable agotamiento de las posibilidades para la realización de la prueba que, en ocasiones, desde un principio se revela ya como en modo alguno factible"*[19].

Las diligencias de investigación que hayan propuesto y llevado a cabo en el proceso donde las partes se encuentren personadas, deberá cumplir una serie de requisitos o exigencias de garantía[20]:

- **Principio de exclusividad jurisdiccional:** correspondiendo al artículo 588 bis de la LECRIM, las medidas mencionadas solo podrán será acordada a petición del MF, la policía judicial, o de oficio por el Juez de Instrucción, cumpliendo ello con la reserva jurisdiccional que marca este principio.

- **Principio de control judicial:** además, la Policía Judicial informará al Juez de Instrucción del progreso de la medida adoptada, con la debida vigilancia que este deberá llevar de aquellas.[21]

[19] Sentencia del Tribunal Supremo de 14 de septiembre de 2006.
[20] PINTO y PALACIOS, F, La prueba en la era digital, Op. Cit,, p 197-
[21] **Artículo 588 bis g LECRIM** - Control de la medida.

- **Principio de especialidad:** este principio preserva una relación entre la medida que se acuerda y medida en curso, en aras de evitar aquello que en derecho conocemos como *"investigaciones prospectivas"***,** y que están prohibidas en nuestro ordenamiento jurídico.[22]

- **Principio de idoneidad:** este principio preserva que la medida cumpla la durabilidad determinada para que sea útil, su buena disposición y capacidad para que cumple el fin determinado.[23]

- **Principio de excepcionalidad:** la medida solicitada y adoptada deberá cumplir dos requisitos en base a este principio, el primero de ellos es que no exista ninguna menos gravosa para la consecución del mismo fin pudiendo preservarse en la medida de lo posible los Derechos Fundamentales del investigado, el segundo requisito cuando este requisito sea idóneo para la investigación del hecho, no siendo posible conseguir esto último sin adoptar dicha medida.[24]

- **Principio de proporcionalidad:** la medida que pueda coartar derechos fundamentales deberá ser tomada bajo este principio de proporcionalidad, es decir, que teniendo en cuenta todas las circunstancias del caso el perjuicio ocasionado a los derechos del investigado no sea mayor que el beneficio que se obtenga de la adopción de esa medida.[25]

"La Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma".

[22] CONFILEGAL "Las investigaciones prospectivas » a ver lo que pesco» están prohibidas en nuestro ordenamiento jurídico", 2020 https://confilegal.com/20190428-las-investigaciones-prospectivas-a-ver-lo-que-pesco-estan-prohibidas-en-nuestro-ordenamiento-juridico/

[23] **Artículo 588 bis a, a apartado 3 LECRIM** – Principios rectores.
"El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad".

[24] **Artículo 588 bis a, apartado 4 LECRIM** – Principios rectores.
"En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:
a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida".

[25] **Artículo 588 bis a, apartado 5 LECRIM** – Principios rectores.
"Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la

4.2.- EL ACCESO DE LAS PARTES A LA INVESTIGACIÓN DE LA PRUEBA ELECTRÓNICA

Las partes personadas en el proceso podrán acceder a los datos incautados en una investigación policial y judicial, siempre y cuando se respeten aquellas premisas que la jurisprudencia del Tribunal Supremo reitera, y es que, el mismo en su Sentencia de 10 de marzo de 2016[26] reafirma que en aquellos dispositivos electrónicos objeto de la investigación, como ordenadores o aparatos de almacenamiento, debe entenderse que anida información y datos personales del investigado susceptible de protección, siendo por ello importante que el acceso a los mismo deba contar previamente con autorización judicial ya sea a las partes o a cualquier funcionario público. Es decir, confiscar cualquier dispositivo con datos personales no legitima el acceder al propio contenido.

Del contenido de esta Sentencia podemos diferencias dos supuestos que tienen virtualidad práctica[27].

1º El acceso a los datos que contengan los dispositivos que se hayan incautado por medio de la entrada y registro a un domicilio. Será el Juzgado de Instrucción mediante auto el que autorice a los agentes el acceso a los datos confiscados en esta entrada y registro, también justificada en ese auto, ya que esta resolución se despliega tanto a la inviolabilidad del domicilio y al derecho a la intimidad.

Para Delgado Martín[28], existen excepcionalidades a estas premisas dictadas por la jurisprudencia, como son las siguientes:

La urgencia por la obtención de los datos, justificable cuando por ejemplo se comenten delitos *"in fraganti"*.

Necesidad de obtener la información, cuando sea estrictamente necesario el registro sin existir una medida menos gravosa para conseguir el fin.

---

gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

[26] STS, Sala de lo Penal, 10 de marzo de 2016, FJ2º (Ponente: Francisco Monteverde Ferrer),

[27] PINTO PALACIOS F y PUJOL CAPILLA P, La prueba en la era digital, Op, Cit p 212-218.

[28] DELGADO MARTÍN J, "Protección de datos personales y prueba en el proceso", Diario La Ley, 2019, p7.

Proporcionalidad en la actuación, es decir, como ya hemos reiterado, que el beneficio por practicarla para el bien social sea mayor que la injerencia del derecho a la intimidad o cualquier otro del investigado.

2º.- El acceso a los datos que contengan los dispositivos que no se hayan incautado por medio de la entrada y registro a un domicilio, los funcionarios de la Policía Judicial deberán poner en conocimiento del Juez de Instrucción del apoderamiento del dispositivo para si cree oportuno acceder a la información que en él se conserve, de la autorización judicial podrá prescindirse siempre y cuando estemos ante algunas de las excepciones que se exponían en el punto anterior.

Y por último, el acceso a los *"cloud computing"* o repositorios telemáticos de datos, se trata de aquellos casos en donde la información se almacena en servidores alojados, conocidos como *"nube"*[29], el propio Juez nuevamente tendrá que valorar y autorizar el acceso a esa información. Cuando se realizan incautaciones de este tipo se deben preservar la integridad de los datos que contenga esa nube para prevenir la no manipulación de su interior.[30]

4.3- LA PERICIAL INFORMÁTICA EN EL PROCESO PENAL

Los informes periciales en la fase de instrucción están regulados en los artículos 456 a 485 de la LECRIM, y recogidos en los artículos 723 a 725 del mismo texto legal para la fase del juicio oral.

Cuando está en curso un proceso penal ordinario o por delito grave en donde se pretende emitir un informe pericial debe hacerse por dos peritos[31], salvo que el Juez considere que uno es suficiente, mientras que en el procedimiento abreviado la regla general es que basta con uno solo.

Cuando el Juez de Instrucción designa a los peritos, puede ser que estos sean recusados por las partes, sin embargo, solo podrá hacerse cuando la prueba no pueda

[29] Un ejemplo de nubes públicas podría ser, Microsoft Azure, Amazon Web Services o Google Cloud.
[30] **Artículo 588 sexies a, apartado 1 LECRIM** – Necesidad de motivación individualizada. *"Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos".*
[31] **Artículo 459 LECRIM** *"Todo reconocimiento pericial se hará por dos peritos […]".*

reproducirse por sí misma en el proceso penal, de lo contrario, esta actuación de recusación quedará limitada[32]. Las circunstancias en las que las partes podrán valerse para que prospere la recusación serán la del parentesco o afinidad con una de las partes involucradas en el proceso, cuando se conozca un interés directo del perito en el proceso, la amistad o enemistad manifiesta, o cualquier otra circunstancia que quede debidamente acreditada y que les haga desmerecer en el ámbito profesional.

Esta recusación podrá valerse en la fase de instrucción, justo antes de que comience la diligencia pericial, debiendo formularse por escrito y aportando los documentos que acompañen a su motivación y justificación, el Juez de Instrucción una vez lo reciba dictará por medio de auto la resolución.[33] En la fase de juicio oral las partes deberán comunicar la recusación una vez se admita dicha pericial y antes de la apertura del juicio oral[34], en los tres días siguientes al que se conozca la identidad de los peritos encargados de este informe, este plazo queda bajo el principio de preclusión ya que aquel perito que no sea recusado en el plazo procesalmente otorgado para ello no podrá serlo después, salvo que pasado este plazo cumpla algunas de las causas de recusación,[35] una vez se da traslado a las partes y se valora la situación se emite auto con la decisión.

En cuando a la aportación de los informes periciales, estos pueden ser aportados por las partes en lo que dure la fase de instrucción, en el proceso ordinario adjuntarlo al escrito de calificación provisional,[36] o aportarlos en el escrito de acusación o defensa en el proceso abreviado,[37] al margen de estas indicaciones los informes periciales en la práctica pueden y suelen presentarse con la querella.

---

[32] **Artículo 467 LECRIM** *"Si el reconocimiento e informe periciales pudieren tener lugar de nuevo en el juicio oral, los peritos nombrados no podrán ser recusados por las partes. Si no pudiere reproducirse en el juicio oral, habrá lugar a la recusación".*

[33] **Artículo 470 LECRIM** *"El Juez, sin levantar mano, examinará los documentos que produzca el recusante y oirá a los testigos que presente en el acto, resolviendo lo que estime justo respecto de la Recusación […]".*

[34]**Artículo 723 LECRIM** *"[…] La sustanciación de los incidentes de recusación tendrá lugar precisamente en el tiempo que media desde la admisión de las pruebas propuestas por las partes hasta la apertura de las sesiones".*

[35] **Artículo 663 LECRIM** *"El perito que no sea recusado en el término fijado en el artículo anterior no podrá serlo después, a no ser que incurriera con posterioridad en alguna de las causas de recusación"*

[36] **Artículo 656 LECRIM** *"El Ministerio Fiscal y las partes manifestarán en sus respectivos escritos de calificación las pruebas de que intenten valerse, presentando listas de peritos y testigos que hayan de declarar a su instancia. […]"*

[37] **Artículo 781 y 784.2 LECRIM** *"[…] En el mismo escrito se propondrán las pruebas cuya práctica se interese en el juicio oral, expresando si la reclamación de documentos o las citaciones de peritos y testigos deben realizarse por medio de la oficina judicial […]"* y *"En el escrito de defensa se podrá*

Independientemente de que las partes puedan aportas sus propios peritos e informes periciales, como se ha visto anteriormente, de oficio por el Juez de Instrucción o a instancia del Ministerio Fiscal puede acordarse la realización de una pericial, en este caso informática, se encargarán de esta práctica habitualmente las Unidades especializadas de la Policía Nacional o Guardia Civil. Los dictámenes que se practiquen durante la fase de instrucción se considerarán diligencias de investigación no pruebas como tales.

Todos los peritos deben, conforme al artículo 474 LECRIM[38], prestar juramento, afirmando que de esta forma desempeñará su función en aras de conseguir la verdad, pudiendo incurrir en responsabilidad penal de lo contrario.

El informe que los peritos aporten al proceso deberá contener lo siguiente, citando textualmente el artículo 478 de la LECRIM:

1.º La descripción de la persona o cosa que sea objeto de este en el estado o del modo en que se encuentren.

2.º La relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.

3.º Las conclusiones que en vista de tales datos formulen los peritos conforme a los principios y reglas de su ciencia o arte.

No hay una forma establecida por la ley para llevar a cabo el examen de los peritos en el proceso, pero conforme a la práctica y a la jurisprudencia podemos asegurar que, una vez los mismos hayan prestado juramento, deberán informar sobre el objeto de la pericia, al mismo tiempo, respondiendo a las preguntas de las partes personadas.

En cuando al valor probatorio, la prueba en el proceso penal se rige por el principio de libre valoración de la prueba,[39] es decir, no existirá ninguna regla para

---

solicitar del órgano judicial que recabe la remisión de documentos o cite a peritos o testigos, a los efectos de la práctica de la correspondiente prueba en las sesiones del juicio oral o, en su caso, de la práctica de prueba anticipada"

[38] **Artículo 474 LECRIM** *"[…] todos los peritos, así los nombrados por el Juez como los que lo hubieren sido por las partes, prestarán juramento, conforme al artículo 434, de proceder bien y fielmente en sus operaciones y de no proponerse otro fin más que el de descubrir y declarar la verdad".*

[39] **Artículo 741 LECRIM** *"El Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley".*

valorarla, entendiéndose que basta con el conocimiento y saber y entender del Tribunal. La prueba pericial informática se valora según estas mismas reglas de la sana crítica, siendo las pruebas que se practican en la fase del juicio oral las únicas pertinentes para desvirtuar la presunción de inocencia, es por ello, que puede a priori parecer que la necesidad de que el perito informático acuda a ratificar su informe pericial, se convierte en un requisito esencial para entrar a valorarla, pero, para la jurisprudencia del Tribunal Constitucional[40] no se considera un requisito indispensable si el informe se ha aportado como veíamos en al fase de instrucción y las partes han tenido conocimiento de esta y no han formulado ninguna impugnación, reconociendo de esta forma una *"aceptación tácita"*, pudiendo valorarse esta prueba aunque no se haya ratificado.

V.- PROBLEMAS JURÍDICOS DERIVADOS DEL USO DE LA PRUEBA ELECTRÓNICA

5.1.- POSIBLE AFECCIÓN A LOS DERECHOS FUNDAMENTALES.

El rápido avance de la tecnología ha conseguido que cada vez más la involucremos no solo como herramienta para facilitar el desempeño de nuestras actividades en el ámbito profesional, sino también en nuestra esfera privada, convirtiendo a muchos de estos dispositivos informáticos que usamos, en *"diarios digitales"*, que almacenan todo tipo de información, algunas de contenido sensible, es por ello por lo que entran en juego las reglas de protección de los derechos fundamentales[41], al considerar el carácter intrusivo que posee este medio probatorio.

Las pruebas derivadas de las nuevas tecnologías es frecuente que puedan vulnerar algunos de los derechos que recoge el artículo 18 de la Constitución Española *(en adelante CE)*, especialmente estos tres derechos:

El derecho a la intimidad[42], ya que se accede a datos personales y sensibles que guardan las personas sobre su esfera íntima.

[40] STC, Sala de lo Penal, de 24 de mayo de 2011, (con remisión a la SS 127/90, 24/91).
[41] PORTAL MANRUBA J, (2013), "La regulación de la prueba electrónica en el proceso penal", Revista Derecho y Proceso Penal, nº3, p 27.
[42] **Artículo 18.1 de la Constitución Española**. "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."

La inviolabilidad del domicilio[43], si el dispositivo se encontrase en un lugar calificado como hogar, salvo que si se haya realizado con consentimiento del perjudicado o autorización judicial.

Derecho al secreto de las comunicaciones[44], ya que muchas de estas pruebas consistirán en interceptar mensajes entre dos o varias personas.

El Tribunal Europeo de Derechos Humanos, (en adelante TEDH), ha sido también tajante en sus sentencias [45]protegiendo la posible afección de estos derechos en el curso de una investigación policial o judicial, necesitando en la mayoría de los casos expresa autorización judicial, sobre todo cuando se trata de utilizar claves o cifrados para acceder a dispositivos que contenga información.

Procede distinguir dos supuestos en cuanto a la afección de estos derechos fundamentales:[46]

En primer lugar, cuando se produce a instancia de parte, cuando una de las partes en el proceso pretende utilizar como prueba la información contenida en algún dispositivo de comunicación, pudiendo contener información cruzadas entre dos o más interlocutores, cuando el que aporta la prueba participa en esa conversación, no estaríamos ante la vulneración de ningún derecho, sin embargo, cuando es un tercero ajeno a este diálogo, y que por tanto no ha participado en la conversación, si se estaría vulnerando un derecho fundamental, como puede ser el secreto de las comunicaciones[47].

En segundo lugar, en el caso de que se produzca de oficio, tanto por parte de los funcionarios de la Policía Judicial como de la autoridad judicial que sea competente, considerando lo dispuesto por la doctrina del Tribunal Constitucional, *"la protección de la intimidad exige regularidad formal de la decisión judicial que motivadamente y con fundamento en una inexcusable previsión legislativa, la delimite sino que también la*

[43] **Artículo 18.2 de la Constitución Española.** *"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".*

[44] **Artículo 18.3 de la Constitución Española.** "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

[45] STEDH de 22 de mayo de 2008, (JUR 2008, 149511) *"Caso Lliya Stefanox contra Bulgaria".*

[46] QUILES MOLLÁ L, *"Las nuevas tecnologías como medio de prueba en el proceso penal"*, Universidad Miguel Hernández, Alicante, 2010, p 40.

[47] STC 11/1989, Sala Segunda de 24 de enero de 1989.

razonable apreciación, por la autoridad actuante, de la situación en que se halle el sujeto que pueda resultar afectado, apreciación que se ha de hacer en relación con las exigencias de la actuación judicial en curso"[48].

Es por ello que la doctrina, en el ejercicio de las funciones de investigación permite que determinadas actuaciones supongan una injerencia para algunos derechos del investigado, siempre en aras de buscar un interés público con la investigación, siendo importante que la medida esté recogida por la ley, debidamente autorizada o justificada, [49] es decir que se respete el principio de proporcionalidad.

5.2.- TEORIA DEL *"FRUTO DEL ÁRBOL ENVENENADO"*, CON APLICACIÓN EN LA PRUEBA ELECTRÓNICA.

Cuando la prueba electrónica aportada no cumple la exigencia de admisibilidad habiéndola obtenido vulnerando derechos fundamentales a terceros, sin pasar con ello los previos controles de legalidad establecido, esta circunstancia recibe por la doctrina, el nombre metafórico de *"la teoría del fruto del árbol envenenado"*, teniendo su origen en el derecho anglosajón conocido en inglés como *"fruit of the poisonous tree doctrine"*[50]. En nuestro derecho esta doctrina se consagró en el año 1984, a raíz de una sentencia del Tribunal Constitucional (STC 114/1984), donde se establece que estas pruebas obtenidas de forma ilícita no deben tenerse en cuenta en el proceso, algo que consagra también el artículo 11.1 LOPJ. [51]

En este caso el árbol correspondería a aquella prueba que se ha obtiene, como decíamos, de forma ilegal o fraudulenta, y en muchos casos vulnerando derechos fundamentales, y el fruto la información que ha descubierto dicha prueba que no podrá tenerse en cuenta, recordemos, ni podrá usarse para que el tribunal entre a valorar el contenido de la prueba propuesta.

---

[48] STC 37/1989, Sala Primera, Rec Recurso de amparo 235/1987 de 15 de Febrero de 1989.
[49] STC 173/2011, de 7 de noviembre, Sala Segunda de 7 de noviembre de 2011.
[50] *"¿Qué es la doctrina del fruto del árbol envenenado y por qué es tan importante para hacer Justicia?"* – CONFILEGAL (2021). https://confilegal.com/20180805-que-es-la-doctrina-del-arbol-envenenado/
[51] **Artículo 11. LOPJ** – *"En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".*

Este precepto trae consigo la adopción de un criterio legal que determina cómo opera con los medios de pruebas obtenidos ilícitamente, reduciendo la incidencia de la decisión judicial sobre la ilicitud de un medio de prueba[52].

El Tribunal Supremo, en su Sentencia 113/2014, 17 de Febrero (FJ 10º), establece que **"***con carácter general, la prohibición de la prueba constitucionalmente ilícita alcanza tanto a la prueba en cuya obtención se ha vulnerado un derecho fundamental como a aquellas otras que, habiéndose obtenido lícitamente, se basan, apoyan o deriven de la anterior, para asegurar que la prueba ilícita inicial no surte efecto alguno en el proceso"*.

Sin embargo, como bien señala la misma Sentencia, el Tribunal Constitucional ha ido matizando la aplicación del artículo 11 LOPJ, como la Sentencia 81/1998, de 2 de abril (FJ 4º), donde desarrolla la doctrina de la conexión de antijuricidad, la cual, supone la existencia de un enlace jurídico entre una prueba y otra, de esta forma, declarada la nulidad de la primera, se produce en la segunda una conexión que la declarar igualmente nula, impidiendo con ello que pueda tenerse en cuenta en el proceso. En este sentido, esta Sentencia sostiene en su FJ 4º, que "*los derechos fundamentales no son ilimitados ni absolutos, por lo que, en supuestos excepcionales, se ha admitido que, pese a que las pruebas de cargo se hallen naturalmente enlazadas con el hecho constitutivo de la vulneración del derecho fundamental por derivar del conocimiento adquirido a partir del mismo, son jurídicamente independientes de él y, en consecuencia, se les reconoce como válidas y aptas*".

5.3.- LA ALTERACIÓN Y FRAGILIDAD DE LA PRUEBA ELECTRÓNICA

Para muchos autores y para el propio Tribunal Supremo[53] este medio de prueba, relativamente joven y tan distinto a los tradicionales que impera en muchos procedimientos hoy en día, posee no solo mucha de ellas una parte material, sino también un *software*, aquella parte intangible que puede ser manipulada o alterada sin dejar huella por las partes del proceso para su propio interés. Sin embargo, existen medidas como ya hemos podido comprobar en algunos epígrafes para blindar estos documentos electrónicos evitando su posible modificación, como pueden ser, darle un

[52] GONGÁLEZ GARCÍA, JM. "El proceso penal español y la prueba ilícita". *Revista de Derecho (Valdivia). Vol. VIII*, nº2, 2015 pp.187-211.

[53] Opinión del TS en la Sentencia 300/2015, de 19 de mayo, que establece: "la posibilidad de manipulación de los archivos digitales mediante los que se materializa el intercambio de ideas forma parte de la realidad de las cosas", FJ 3.

mayor protagonismo la firma digital garantizando con ello una mayor dificultad a la hora de alterar el documento o al menos descubrir que el mismo ha sido alterado, el auxilio fundamental de los peritos informáticos especializados en soportes digitales que constaten la autenticidad de las pruebas en el proceso.

5.3.1.- MEDIDAS PARA CONSERVAR LA PRUEBA ELECTRÓNICA

Uno de los inconvenientes de la prueba digital es la facilidad de alteración de esta, por su volatilidad lo que dificulta a los abogados de ambas partes a conservar su originalidad y ser calificada por el Tribunal como se espera.

La carta para la preservación del patrimonio digital redactada por la UNESCO[54], contribuyen a esta preservación, definida como todos aquellos procesos destinados a garantizar la conversación de un contenido digital. Los métodos más utilizados a los que pueden recurrir los abogados proteger esta prueba son:

- **La preservación de los sistemas originales:** Se preservar el software o entorno donde estos datos han sido creados manteniéndolo en funcionamiento para evitar su obsolescencia. El inconveniente de este método es el coste que supone de equipamiento.

- **Migración:** Consiste en un cambio o evolución de versiones hacia un sistema mejorado, este método convierte la información de un formato a otro, convirtiéndolos tanto desde un software o hardware a otro distinto, consiguiendo que conserven sus características originales. Este conjunto de tareas consigue la transferencia periódica de material digital, preservando de este modo la información y permitiendo que se puedan recuperar los datos necesarios desde una generación tecnológica a otra. La migración es un método muy usado en la práctica, ya que los conocimientos técnicos que se necesitan saber son muy básicos y escasos permitiendo con ello poder acceder a ella con facilidad, la mayoría del proceso se automatiza, sin embargo, el inconveniente que plantea este procedimiento es que no es recomendable para datos que se encuentren en distintos formatos ya que hará falta que cada uno de estos reciba un tratamiento

[54] https://unesdoc.unesco.org/ark:/48223/pf0000130071_spa

distinto, no se puede confirmar que realmente el documento original no se encuentre alterado, este proceso deberá repetirse frecuentemente a lo largo de la vida tecnológica del formato.

- **Emulación:** Una alternativa a la migración, este método convierte el entorno en el que se encuentra el documento para poder leer su original, simulando este, para conservar recursos digitales más completos, compatibilidad de formatos, un ejemplo de ello podrían ser documentos rescatados en investigaciones que duran años y cuyos softwares se han quedado obsoletos, permitiendo esta medida poder leerlo en soportes más modernos, y actualizados.

- **Copia de Seguridad:** Consiste en un proceso de duplicación de un documento o archivo digital, que disminuya el riesgo de pérdida o extravío. En cualquier caso, esto no produce la conservación segura de dicho documento o archivo, pues, lo único que hace es multiplicarlo, para poder conservarlo, por ejemplo, en otro espacio digital o en algún dispositivo de almacenamiento de datos. No obstante, una copia digital asegura en mayor medida la posibilidad de incorporarlo en el proceso y que no desaparezca, sin embargo, es vital prestar una atención especial al equipo informático o el medio digital donde se quiere conservar, teniendo en cuenta que éste sea seguro, y mejor aún, personal.

- **Replicado y rejuvenecimiento:** El replicado consiste en duplicar una base de datos de forma que se encuentre repetido en otra localización digital (pág 120, Piñeiro). Este proceso tal y como establece el autor, permite una mayor disponibilidad de los datos. Es una operación que están llevando a cabo la mayoría de empresas que manejan una gran cantidad de datos, ya sean propio o de clientes, de forma, que se garantice una mayor seguridad de conversación ante posibles ataques o daños informáticos. De igual forma, por el deterioro del equipo informático donde se encuentran esos datos.

  Por lo tanto, como ya se dijo anteriormente, se trata de otra forma de preservar dicha información y como tal, el medio de prueba en el procedimiento penal.[55]

[55] PIÑEIRO GÓMEZ, JM "Base de datos relacionales y modelado de datos". Ediciones paraninfo, S.A. 2013.

- **Preservación en línea:** Consiste en almacenar la información en una nube en lugar de utilizar soportes físicos como discos duros, ahorrando con ello copiar los datos de un lugar a otro y siendo más fácil acceder a ella, la problemática de este método es que, si se pierde el servidor, no existirían más copias.

- **Arqueología digital:** Intenta recuperar archivos que estén almacenados en sistemas dañados (discos duros rotos, que se han intentado borrar...), obsoletos (como disquetes), corrompidos o encriptados (si existe un archivo protegido por una contraseña que no se conoce, útil también en las situaciones en las que un ransomware daña y encriptar este archivo impidiendo su lectura pudiendo probar a ejecutar algunos algoritmos para intentar desencriptarlo.

Los principales objetivos de este trabajo eran conocer las cuestiones relevantes que pueden surgir desde un punto de vista jurídico cuando proponemos en el procedimiento penal una prueba calificada como electrónica, con las peculiaridades que la misma entraña y con esto hemos llegado a las siguientes conclusiones frente a los numerosos inconvenientes que como hemos tenido la ocasión de ver plantean muchos autores sobre el uso de este tipo de prueba:

1.- La prueba electrónica puede ser por supuesto, objeto de manipulaciones, pero de la misma forma que una prueba convencional sufre este riesgo, ya que los medios tecnológicos son tan amplios hoy en día que han conseguido que ninguna prueba pueda escapar de esta posibilidad, en embargo, aquella prueba que ha sido generada por un medio tecnológico ofrece una información mas precisa y completa contando además con determinadas técnicas como ya hemos comprobado para preservar su integridad.

Quizá lo más acertado para esto sería reproducir la prueba en su medio digital natural, cotejando el Letrado de la Administración de Justicia o el propio Tribunal su veracidad, algo que podría salvar la posible manipulación ya que las pruebas digitales aportadas como pruebas se acaban convirtiendo en la práctica a un formato papel convencional.

2.- La evolución tecnológica ha provocado que estas pruebas digitales estén al orden del día en los procedimientos de todas las jurisdicciones, no solo en la que nos hemos centrado en este trabajo. Una razón más para conseguir la digitalización de la Administración de Justicia o que la misma apueste por medios tecnológicos.

3.- Existe la problemática de la brecha tecnológica en los profesionales del sector, que podría solucionarse recibiendo la formación adecuada para implicar el uso de medios tecnológicos de los que no podemos evitar. La Administración de Justica podría nutrirse de profesionales informáticos que comprueben las pruebas aportadas por las partes, estudiando su lenguaje

informático para evitar las alteraciones y asegurar la autenticidad de todo lo que en fase probatoria se presenta, así como servir de auxilio al resto de funcionarios de justicia para incorporar el conocimiento más complejos o técnicos que se requieran en el uso de estos medios digitales.

4.- Por otro lado la magnitud a la que hay llegado los dispositivos digitales a adentrarse en nuestras vidas, han conseguido que cada vez exista más acceso a los datos e información que engloban la esfera privada e intima de las personas, vulnerando con ello muchas veces derechos fundamentales, que no podemos olvidar merecen una protección especial.

Cierto es que las nuevas tecnologías, han conseguido entorpecer algunos de los aspectos personales de nuestras vidas, sim embargo, valorando la cara positiva y el gran crecimiento y protagonismo que tienen las mismas hoy en día, hay que conseguir integrarlas en los aspectos jurídicos que nos rodean como lo hemos hecho en nuestra vida diaria, en esta carrera contra las nuevas tecnologías el legislador sigue yendo en segundo puesto.

BIBLIOGRAFÍA

- ABEL LLUCH X, “La prueba documental”. Colección de formación continua Facultad de Derecho ESADE, Madrid, 2010, Serie estudios prácticos sobre los medios de prueba, p 30.
- ABEL LLUCH X, La prueba electrónica, series estudios prácticos sobre los medios de prueba, ESADE, Madrid, 2011, p 27-29.
- CONFILEGAL – “Las investigaciones prospectivas –» a ver lo que pesco» están prohibidas en nuestro ordenamiento jurídico”, 2020.
- CONFILEGAL “¿Qué es la doctrina del fruto del árbol envenenado y por qué es tan importante para hacer Justicia?”, 2021
- DELGADO MARTÍN J, La prueba electrónica en el proceso penal, Diario La Ley, número 8.167, 2013 p I.
- DELGADO MARTÍN J, “La prueba del Whatsapp”, Diario La Ley, nº 8605, Sección Tribuna, 15 de septiembre, 2015.
- DELGADO MARTÍN J, “Protección de datos personales y prueba en el proceso”, 2019 p7.
- GIMENO SENDRA, J V, Derecho Procesal Penal, Editorial Aranzadi, Madrid, 2020, p 371.
- GONGÁLEZ GARCÍA, JM. “El proceso Penal español y la prueba ilícita”. *Revista de Derecho (Valdivia). Vol. VIII*, nº2, 2005, pp.187-211.
- HERNÁNDEZ DIAZ L, “El delito informático”, Eguzkilore, País Vasco, 2009, p.230-232.
- PINTO PALACIOS F y PUJOL CAPILLA P, La prueba en la era digital”, Wolters Kluwer, Madrid, 2017 p 38-62.
- PIÑEIRO GÓMEZ, JM , Base de datos relacionales y modelado de datos. Ediciones paraninfo, S.A, 2013.
- PORTAL MANRUBA J, “La regulación de la prueba electrónica en el proceso penal”, Revista Derecho y Proceso Penal, nº3, 2013, p 27.
- QUILES MOLLÁ L, “Las nuevas tecnologías como medio de prueba en el proceso penal”, Universidad Miguel Hernández, Valencia, 2016, p 40.
- SAEZ-SANTURTÚN PRIETO M, La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 mayo de 2015, Diario La Ley, 2015, nº 8.637
- SIMON KEMP, “Digital 2021: Global overview report”, Datareportal. 2021.
- VERA DELFA C, El correo electrónico: el nacimiento de un nuevo género, Tesis Doctoral, Facultad de Filología, Universidad Complutense de Madrid, Madrid. 2006.