2.3. LOS DISTINTOS TIPOS DE PRUEBA TECNOLÓGICA.

El concepto de prueba de las nuevas tecnologías o electrónica abarca las generadas de forma directa por medio de la informática, las que proceden de documentos electrónicos y las que se encuentran en elementos externos pero que guardan relación o similitud con las características de un soporte electrónico o informático.

Por tanto, entendemos que existen una gran variedad de medios probatorios tecnológicos, que se encuentran en constante movimiento e innovación ya que dependen de los avances que se produzcan en las nuevas tecnologías.

A título ejemplificativo, se explicarán las pruebas tecnológicas más comunes en los procesos penales: [30]

1. Correo electrónico: se encuentra definido en la Directiva 2002/58 del Parlamento Europeo y Consejo, en particular, en el artículo 2 h): "todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo." Se trata de un servicio que hoy en día se ha convertido de uso habitual y nos permite la comunicación con cualquier persona a cualquier distancia de forma inmediata.

2. *SMS y MMS* de los teléfonos móviles: consiste en un sistema de mensajería que permite enviar y recibir mensajes de texto, en el caso de los *SMS*, e incluso acompañado de imágenes, sonido o vídeos y similares en el caso de los *MMS* que permite a los teléfonos móviles utilizar este tipo de comunicación. Tienen un tratamiento muy similar al del correo electrónico. Aunque, actualmente, está disminuyendo su uso, están presente como prueba en el proceso penal.

3. Foros, redes sociales, chat, blogs: se tratan de lugares virtuales que se utilizan para introducir las ideas, pensamientos, *hobbies* o similares en el cual pueden

[30] http://docplayer.es/1080774-Facultad-de-derecho-departamento-de-criminologia-15-de-marzo-de-2013-la-prueba-electronica-en-el-proceso-judicial-ventajas-e-inconvenientes.html (consultado el 24 de marzo de 2016)

intercambiar opiniones, experiencias o pensamientos sobre distintos temas. A su vez, nos permite comunicarnos con personas de diferentes partes del mundo. Así entendemos que la utilización de estos medios de comunicación telemática se puede producir fácilmente la vulneración del derecho a la intimidad o al secreto de comunicaciones e incluso a la protección de datos por parte de terceros.

4. Aplicaciones para *Smartphones* o *tablets* tales como *WhatsApp, Telegram* entre otras: consisten en aplicaciones de mensajería instantánea que permite el envío de mensajes de texto, imágenes, sonido, vídeos con los números de teléfonos que se encuentren en los dispositivos. Las conversaciones mantenidas a través de las mismas cada vez son más frecuentes en los procedimientos judiciales.

5. DNI electrónico: sirve para todo tipo de tramitación telemática que abarca actividades como presentar la declaración de la renta, la realización de transacciones como empresas, entre otras más.

Todas estas pruebas tecnológicas tiene en común las disposiciones que contempla la Ley 25/2007, de 18 de octubre de conservación de datos relativa a las comunicaciones electrónicas y a las redes públicas de comunicaciones nace de acuerdo con la Directiva 2006/24 CE del Parlamento Europeo y del Consejo de 15 de marzo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones que tiene por objeto establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos con el fin de posibilitar que dispongan de ellos agentes facultados, así como, el deber de cesión de los mismos a éstos siempre que les sean requeridos mediante autorización judicial con fines de detención, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2.4. LA ADMISIÓN, APORTACIÓN Y VALORACIÓN DE LA PRUEBA TECNOLÓGICA.

2.4.1 La admisión de la prueba.

Una vez propuesta la prueba por las partes o de oficio se procede a la admisión o inadmisión de la misma. Hoy en día, no existe una regulación específica de la admisibilidad de la prueba de las nuevas tecnologías lo que nos obliga a remitirnos a las disposiciones generales reguladas en la LEC.

Para que una prueba sea admitida, ha de cumplir con los siguientes criterios: el de pertenencia, utilidad, licitud e idoneidad.

1. Entendiendo por pertenencia aquella prueba que tenga relación, ya sea directa o indirecta, con el objeto del proceso.

2. Por utilidad que sea relevante para la clarificación de los hechos que se investigan y que sean necesarias atendiendo a sus resultados.

3. Entendiendo por lícita aquella que se ha obtenido sin vulnerar los derechos fundamentales o sin contravenir las disposiciones legales vigentes.

4. La idoneidad de la prueba, es decir, que sea presentada a través de un medio de prueba adecuado, aquél que no se encuentre prohibido en vía procesal.

2.4.2. La aportación al proceso.

A pesar de la reciente modificación de la Ley de Enjuiciamiento Criminal y su inclusión de las nuevas tecnologías en el proceso penal, a día de hoy, como ya se ha dicho en el apartado anterior, aún nos encontramos con la inexistencia de un precepto legal en el que se establezca una referencia a cómo y cuándo aportar la prueba tecnológica al proceso, obligándonos a acudir a las normas que rigen con carácter general la aportación de la prueba en juicio. Como consecuencia de ello, nos vemos obligados a acudir a las disposiciones generales de la práctica de la prueba establecidos

en la Ley de Enjuiciamiento Civil, en particular, al artículo 299.2 que regula los distintos medios de prueba de los que pueden valerse las partes, como prueba documental ya sea pública o privada, como prueba pericial, estos dos medios de prueba son los más usuales pero también puede darse incluso como prueba testifical o interrogatorio de las partes entendiendo por ésta el testimonio de una persona que ha tenido contacto con el dispositivo.

En primer lugar, hay que tener en cuenta que la forma más habitual de introducir al proceso penal estas fuentes de prueba mediante una prueba documental pública o privada y/o acompañada de una pericial.

En segundo lugar, también cabe la posibilidad de aportar la prueba en el soporte telemático que se encuentre, éstos gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales[31] . Entendiendo por autenticidad, aquella prueba que se considera que expresa certeza y realidad de los datos que en la misma se contiene y, entendiendo por integridad, aquella que se incorpora al proceso en su totalidad y sin haber sido alterado. Por tanto, una buena forma de garantizarlo es a través de una diligencia de cotejo realizada por el Letrado de la Administración de Justicia en la que se levante acta de constancia en la que el mismo dé fe pública del documento o por medio de un Notorio dé fe pública notarial de los datos contenidos en el soporte y en la transcripción.[32]

En relación con la fe pública judicial, el Letrado de la Administración de Justicia tiene la posibilidad de dar o no fe pública, como fedatario público, de la veracidad y autenticidad de la información que sea objeto de prueba que se encuentre en un dispositivo electrónico. Al referirnos a que puede no dar fe pública sobre estos documentos que se encuentran en formato digital, estamos haciendo reseña a que esta diligencia de constancia no se encuentra regulada en ningún cuerpo normativo. Por tanto, a la hora de solicitar la diligencia de cotejo de la prueba electrónica en cuestión ante el Letrado de la Administración de Justicia, cabe la posibilidad de que se dé alguna

[31]Véase en la STS 1066/2009, de 4 de noviembre.
http://supremo.vlex.es/vid/-231838650 (consultada 26 de marzo de 2016)
[32]Véase en la Sentencia de la AP de Córdoba 159/2014 de 2 de abril 2014.

de las siguientes situaciones: a) que levante acta de constancia del documento aplicando la legislación actual correspondiente según su criterio, b) que inste ciertos requisitos para efectuar dicha diligencia y c) que se niegue a efectuarla. [33]

En relación con la fe pública notarial, en disonancia con lo anterior, cualquier Notario levantará acta de constancia de los datos que se encuentren en dispositivos electrónicos ya que así se encuentra regulado legalmente en la Ley Notarial (LN), en el precepto 17 bis. Ha de disponer del dispositivo electrónico o estar en presencia de dónde se encuentra el texto digital y será a partir de aquél momento en el que podrá proceder al cotejo del contenido con la finalidad del levantamiento de acta posterior. A su vez, será necesario para ello, las claves de acceso del soporte electrónico. En dicha acta, constarán todos los datos íntegros que sean determinantes para certificar su autenticidad o falsedad del documento.[34]

Por un lado, en cuanto a la cuestión relativa a cuándo se aporta, de acuerdo con los criterios generales, se practicará durante la fase de instrucción por cualquier de las partes que podrán aportar una prueba tecnológica solicitando su adhesión a los autos del soporte electrónico o informático en el que se encuentra la misma, de tal manera que el mismo pueda ser reproducido en juicio oral, acompañándose de una copia en papel con la transcripción de la información o hechos relevantes que contenga para el delito investigado. A continuación, el Juez de Instrucción correspondiente, podrá, siempre y cuando, sea relevante para el esclarecimiento de los hechos, decretar la práctica de una diligencia de investigación de carácter tecnológico mediante la correcta orden judicial motivada en el que se indiquen los motivos, el lugar que la ha motivado. [35]

[33]PUJOL CAPILLA, P., *La nueva prueba documental en la era digital. Su valoración en juicio.* Editorial Jurídica Sepín, Madrid 2014., pp. 36 a 40.
[34]PUJOL CAPILLA, P., *La nueva…", Op. Cit.,* pp. 41 a 44.
[35] Véase en Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial LA LEY https://peritoit.files.wordpress.com/2013/10/la-prueba-eletronica-en-el-proceso-penal.pdf (consultada el 25 de marzo de 2016)

Por otro lado, en cuanto a cómo han de ser aportados en el proceso penal, reciente jurisprudencia ha establecido una serie de criterios de cómo aportar este tipo de pruebas[36]:

A) Cualquiera de las partes podrá aportar al proceso penal la transcripción de una comunicación a través de la aportación de una copia de la conversación mantenida a través de un dispositivo electrónico junto con el soporte en cuestión.

B) En el caso de que no procede la impugnación que los documentos aportados tales como las copias o fotocopias de las conversaciones no sean impugnados por la contraparte, de este modo, podrá adquirir valor probatorio junto con el resto de pruebas debidamente aportadas al proceso.

C) Si la contraparte lo impugna le corresponderá la carga de la prueba a quien la aportó y la introdujo al proceso habrá de mostrar su autenticidad y la originalidad del documentos para que alcancen valor probatorio.[37]

En estos casos, lo más conveniente para garantizar la absoluta veracidad y autenticidad del documento, consiste en la práctica de una pericial informática que la realice un técnico informático especializado que examine el dispositivo o el soporte electrónico y practique las diligencias necesarias para ello.

2.4.3. La valoración judicial.

El Juez competente tendrá que tener en cuenta para la correcta valoración de la prueba: la integridad y autenticidad de la misma, la postura procesal que hayan tenido las partes, es decir, si ha sido impugnada o no y la valoración conjunta de todas las pruebas practicadas en el acto del juicio oral en el proceso penal.

---

[36]FUENTES SORIANO, O., "La intervención de las comunicaciones tecnológicas tras la reforma de 2015*" en VVAA, Jornadas sobre la reforma de la Ley de Enjuiciamiento Criminal*. Primer Memorial Prof. Dr. Manuel Serra Domínguez (en prensa)., p.17.
[37]Véase en la STS (penal) 300/2015, de 19 de mayo.

Con todo ello, hay que tener en cuenta, el principio que rige a la hora de la valoración de la prueba en el proceso penal regulado en el art. 741 LECrim se refiere a que "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." Del que se desprende la libre valoración de la prueba que tienen los Jueces. Entendiendo por la libre valoración de la prueba, que la ley no obliga al Juez a tener por probados hechos que se presenten en la prueba electrónica, es decir, que el Juez valorará la prueba conforme a las reglas de la sana crítica de acuerdo con criterios racionales atendiendo a la particularidad del caso y de la prueba aportada ajustado siempre a las reglas del derecho.

Con respecto a la posición de las partes en el proceso, si no se produce impugnación de la autenticidad e integridad de la prueba electrónica, el Juez la entenderá como auténtica e íntegra y la valorará conforme a las reglas de la sana crítica. Y si se impugna por alguna de las partes el Juez la valorará de acuerdo con las alegaciones que fundamenten su impugnación y de lo que se desprenda del informe que se emita tras la práctica de la prueba pericial en el que se determine si la prueba es auténtica e íntegra e incluso. En la misma línea, el Juez valorará si las disposiciones que el perito ha emitido en su informe, así como las conclusiones que en el mismo versan que no ha existido manipulación o alteración alguna en el soporte electrónico en el que tuvo lugar la conversación y la réplica que se haya aportado al proceso.

Por ello se observa, que la autenticidad del origen y la originalidad de la prueba, serán elementos que incidirán de manera notoria en la valoración de la prueba tecnológica.

Sin embargo, como bien establece FUENTES SORIANO en ciertos casos se puede dar que a la hora de la impugnación de la prueba no haya posibilidad de practicar pericia informática alguna. Así pues, tendrá la consideración de prueba indiciaria. Asimismo dispone que "en tales supuestos, la fotocopia aportada con la comunicación podrá constituir un indicio más de la comisión del hecho delictivo de forma tal que, según los criterios de la prueba indiciaria: a) por sí sola no puede dar cuenta de la comisión del delito; b) pero unido a otros indicios que resulten probados y se encaminen al mismo resultado probatorio, y valorados todos ellos en su conjunto – ahora sí- según

las reglas de la sana crítica y la aplicación de máximas de experiencia, el Juez podrá dar por probado el hecho sin necesidad de dictamen pericial."[38]

La resolución judicial que adopte el Juez ha de ser motivada, en la que se pondere los medios de prueba que han sido practicados durante el acto del juicio oral y que se determinen en las razones por las que se adoptan la decisión.[39]

3. EL CORREO ELECTRÓNICO COMO PRUEBA JUDICIAL

3.1. Consideraciones generales.

A la vista de los grandes avances tecnológicos producidos en la sociedad durante las últimas décadas han surgido nuevos sistemas de comunicación y formas de relacionarse produciéndose inevitablemente el fomento del uso de las comunicaciones telemáticas. Entendiendo, de este modo, a Internet, como el principal desencadenante y transmisor de información.

Existen múltiples formas telemáticas para comunicarse a nivel mundial como nacional, siendo una de las más relevantes e incluso la más utilizada en la actualidad, el correo electrónico. Así lo establece PUJOL CAPILLA,[40] al decir que "este sistema de comunicación es, en la actualidad, el más extendido entre las personas, tanto en el terreno laboral como en el profesional, además de ser el más antiguo." Y como bien hace referencia, "además de ser el más antiguo" a causa de que las comunicaciones efectuadas por el medio telemático del correo electrónico son semejantes a las del correo postal, de modo que, es de aplicación el mismo tratamiento procesal, en otras palabras, no podrán intervenirse la correspondencia tanto de persona física o jurídica, excepto que medie una autorización judicial.

[38]FUENTES SORIANO, O., "Comunicaciones..." Op. Cit., p.16.
[39]PORTAL MANRUBIA, J., "La regulación de la prueba electrónica en el proceso penal", BIB 2013/1452, Revista Aranzadi de Derecho y Proceso Penal núm. 31/2013, Editorial Aranzadi, SA., p.20.
[40]PUJOL CAPILLA, P., *La nueva…."Op. Cit.*, pp. 9-11.

Por lo que se refiere a la concepción del correo electrónico, se acude a lo dispuesto en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, en concreto, en su artículo 2 h): "todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones públicas que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo."

El correo electrónico es un medio de comunicación mediante el que se permite el intercambio de textos digitalizados tales como imágenes, videos, audios, etc. Su funcionamiento es similar al del correo postal ya que ambos posibilitan la recepción y emisión de mensajes al lugar de destino gracias a la existencia de una dirección, pero con la gran ventaja de que nos permite una recepción prácticamente a tiempo real o diferido del correo, siempre y cuando, se tenga acceso a la conexión de Internet, independientemente del lugar que se encuentre el remitente y el destinatario. Pero, a su vez, tiene un claro inconveniente, se trata de la gran facilidad de manipulación de este tipo de mensajes ya que puede no ser enviado por el emisor que figura en la dirección del correo electrónico, que puede ser suplantado por otra persona e incluso puede construirse un documento con apariencia de correo electrónico totalmente ficticio.

Como consecuencia de la masiva utilización de este medio de comunicación, tanto a nivel interpersonal como profesional, cada vez son más frecuentes la presencia de los correos electrónicos en los procesos judiciales para que sean aceptados tales como prueba electrónica o de las nuevas tecnologías. Por ello, diversos expertos en Derecho establecen la necesidad conservar los mensajes que sean recibidos a través del correo electrónico como PUJOL CAPILLA [41] "es necesario guardar los mensajes recibidos durante algunos años, sobre todo los de cierta transcendencia y que podamos necesitar más adelante."

[41]PUJOL CAPILLA, P., *La nueva..." Op. Cit.*, pp. 9-11.

De acuerdo con la utilización cada vez más frecuente de los correos electrónicos en los procesos judiciales alude FUENTES SORIANO[42] que "un correo electrónico puede ser el objeto mismo el delito, puede ser exclusivamente la fuente probatoria de la comisión de un delito o puede ser, además del objeto mismo del delito, la prueba de dicho delito."

Cualquier correo electrónico puede ser aportado como prueba en juicio con independencia del carácter de su contenido. Otra cuestión diferente, es que se le adquiera por parte del Juez valor probatorio que dependerá de la licitud de la fuente probatoria como de la relevancia que tenga el mismo para el caso que respalde que sea objeto de enjuiciamiento. Así pues, la mejor de las garantías para que los correos electrónicos alcancen pleno valor probatorio se trata de la necesidad de que se cuente con el acceso al original.[43]

Por otro lado, cabe entender por lícitos, aquellos correos electrónicos que han sido aportados con el consentimiento de los partícipes, que hayan sido los mismos participantes del hilo de la comunicación telemática los que la hayan aportado o que medie la autorización judicial debidamente motivada. Del mismo modo, para que el correo electrónico sea una prueba electrónica admisible en juicio es necesario asegurar la totalidad, plenitud e integridad de los soportes de almacenamiento digital o electrónico tales como *Smartphone,* ordenadores*, tablets*, etc., dónde se haya enviado o recibido dicho correo que se aporta.

La aportación de los correos electrónicos que se presentan como prueba en juicio,puede conllevar a acabar con la privacidad de las personas amparada por la Constitución como derecho fundamental en su artículo 18, que abarca la intimidad personal y familiar, la propia imagen y el secreto de las comunicaciones que trataremos a continuación en el siguiente apartado de manera detallada así como dando indicaciones de qué hacer en los casos que dicha privacidad sea vulnerada y la actuación de los poderes públicos en tales casos.

[42] FUENTES SORIANO, O., "El valor probatorio de los correos electrónicos", en ASENCIO MELLADO (Coord.), *El proceso penal ante nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, en prensa., p.4.
[43] MENÉNDEZ, L., "Nuevos tiempos, nuevas pruebas." Escritura Pública, núm. 83, septiembre/octubre de 2013, pp.16-18.

3.2. LA VULNERACIÓN DE LOS DERECHOS FUNDAMENTALES.

Como bien se ha dicho, en el último párrafo del apartado anterior, con la aportación de los correos electrónicos como prueba electrónica al proceso judicial, es frecuente que se produzca la violación de los derechos fundamentales que se encuentran regulados en el art.18 CE. En el caso de que se produzca efectivamente tal violación la prueba de las nuevas tecnologías devendrá en prueba prohibida como así lo dispone el artículo 11 de la LOPJ.

Los derechos fundamentales consagrados en dicho artículo, que se encuentran frecuentemente en "peligro" con el uso en juicio del correo electrónico como prueba judicial, son especialmente el derecho a la intimidad, tanto personal como familiar y al secreto de las comunicaciones.

Si examinamos detalladamente la posibilidad de vulneración del derecho a la intimidad, personal o familiar, cabe destacar su protección a parte de en el artículo 18.1 de la Constitución y en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal o familiar y a la propia imagen, la misma en su artículo 7, dispone que se entiende por intromisión ilegítima de tal derecho:

"1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.

4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.

6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.

7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas."

Dentro del cual, se incluye la posibilidad de que la presentación de una prueba tecnológica, tal y como es el correo electrónico, que incida o invada en uno de los ámbitos que señala este artículo. Estaría violando tal derecho, a la vez, que incurriría en un delito contra la intimidad regulado en el art. 197 CP.

A diferencia del derecho al secreto de las comunicaciones, contiene una especial protección de las comunicaciones las que habrán de ser protegidas con independencia de su contenido. De acuerdo con el alcance del mismo, cubre tanto el contenido de la comunicación como la identidad subjetiva de los interlocutores o de los corresponsales. A la vez, que ha de fijarse cuáles son los límites temporales de protección del precepto 18.3 CE únicamente se protege la comunicación, con independencia del carácter del contenido, entendiendo tal protección desde que comienza hasta que termina la misma, de tal forma que, en el caso de que se produzca una afectación a un derecho fundamental que tenga relación con la comunicación pero que no pertenezca a la

duración de la misma, se estarán infringiendo otros derechos fundamentales tal y como el derecho a la intimidad de distinta protección que el del secreto a las comunicaciones.

Debemos distinguir dos casos en cuanto a la vulneración de los derechos fundamentales:

1) En el caso que produzca a instancia de parte, es decir, que sea una de las partes la que pretenda hacerse valer como prueba judicial que tenga por objeto el contenido de una conversaciones mantenidas a través del correo electrónico por alguna de las partes que fueran interlocutoras de la comunicación mantenida a través del mismo, no se vulneraría en caso alguno el derecho a la intimidad ni el derecho al secreto de las comunicaciones ya que el contenido de dicha conversación convertiría su carácter en público habilitando de este modo la intervención de su contenido por parte de la policía judicial o por terceras personas tales como peritos, entre otros.[44] A la vez que tampoco incurrirá en un delito contra la intimidad de la persona regulado en el art.197 CP.

Sin embargo, en caso que sea un tercero el que aporte como prueba un correo electrónico de cuya conversación no haya sido partícipe estará vulnerando en tal caso el derecho al secreto de las comunicaciones. Asimismo lo dispone la doctrina constitucional[45] "quien graba una conversación de otros, atenta, independientemente de toda consideración, al derecho reconocido en el art. 18.3 CE; por el contrario, quien graba una conversación con otro incurre, por ese solo hecho, en conducta contraria al precepto constitucional citado."

2) En el caso de que se produzca de oficio, ya sea por la autoridad judicial competente o por la Policía Judicial, habrá que atender a lo siguiente:

- De acuerdo con la doctrina constitucional que hace referencia al derecho a la intimidad[46]: "la protección de la intimidad exige regularidad formal de la decisión

[44] GONZÁLEZ I JIMÉNEZ, A., *Las diligencias policiales y su valor probatorio*, BOSCH, 2014, pp. 241 y 242.
[45] Véase en la STC 11/1984.
[46] Véase en la STC 37/1989.

judicial que motivadamente y con fundamento en una inexcusable previsión legislativa, la delimite sino que también la 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."

Teniendo en cuenta que, el art. 18.1 CE no prevé garantía de autorización judicial respecto de las intervenciones que afectan al derecho a la intimidad, de este modo, en ciertos casos de manera totalmente excepcional de acuerdo con la jurisprudencia constitucional se ha admitido con la suficiente y precisa habilitación legal que se puedan practicar en el ejercicio de sus funciones de investigación determinadas actuaciones que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial siempre que se hayan respetado el principio de proporcionalidad. Y encontramos esa previsión legal que permite la injerencia al derecho a la intimidad sin autorización judicial, en los preceptos 7 y 8 de la LO 7/1986 y los arts. 282, 292, 789.1 y 3 LECrim.

Ahora bien, la jurisprudencia del TC alude, con respecto, a los requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia policial en el derecho a la intimidad: " a) la existencia de un fin constitucionalmente legítimo, considerando como tal el interés público propio de la prevención e investigación del delito y más en concreto la determinación de hechos relevantes para el proceso penal, b) que la medida limitativa del derecho a la intimidad esté prevista en la ley principio de legalidad c) que en caso de no contar con autorización judicial o consentimiento del afectado, la actuación policial que atenga a la habilitación legal teniendo en cuenta que la ley puede autorizar a la policía la práctica de inspecciones, reconocimientos e incluso intervenciones corporales leves, siempre y cuando, se respete el principio de proporcionalidad, concretado en tres exigencias o condiciones; idoneidad de la medida, necesidad de la misma y juicio de proporcionalidad en sentido estricto"[47].

En definitiva, la regla general en relación al derecho a la intimidad, se llevará a cabo su limitación con la autorización judicial motivada, siempre y cuando, se acorde con el principio de proporcionalidad. En el caso de que no se dé la misma, toda medida

[47] Véase en la STC 173/2011, de 7 de noviembre.

que se tome que afecte a la esfera de lo íntimo ha de ponerse a disposición judicial para que él tome directrices. Existe, una excepción relevante, consiste que en los supuestos que concurra razones de urgencia y necesidad la Policía sin la preceptiva autorización judicial respetándose de este modo inclusión el principio de proporcionalidad o que exista una habilitación legal para tales casos, que las hay.

- Por otro lado, el derecho al secreto de las comunicaciones, tiene un tratamiento de protección constitucional distinto, como dispone la jurisprudencia del Tribunal Constitucional [48]: "(...) cabe recordar que este Tribunal ha señalado si bien de conformidad con el art 18.3 CE, la intervención de las comunicaciones ya sea postales, telegráficas o cualquier otras, requiere siempre de autorización a menos que medie el consentimiento previo del afectado."

Aunque en el art. 18.3 CE se disponga expresamente la mención de las comunicaciones postales, telegráficas o telefónicas, no hay que entender que se trata de una lista cerrada, sino que cabe entender dentro de este precepto la inclusión de comunicaciones telemáticas tal como los correos electrónicos, siempre que hayan tenido lugar a través de algún soporte técnico, debido a que en el caso de que se dé la presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación, en consecuencia, en el caso de que se produzca la divulgación del secreto por uno de los interlocutores no se considera violación del art. 18.3 CE, sino, en su caso, vulneración del derecho a la intimidad.[49]

En concreto, el caso de las comunicaciones postales, queda garantizado tanto el contenido de la comunicación como los datos que contesten en la dirección tanto de recepción como de envío. Ahora bien, tal y como señala la jurisprudencia del Tribunal Constitucional[50] el art. 18.3 de la CE solamente es objeto de protección el secreto de las comunicaciones postales.

[48] Véase en la STC 115/2013, de 9 de mayo.
[49] Véase en la STC 114/1984.
[50] Véase en la STC 281/2006, de 9 de octubre.

Por tanto, el artículo 18.3 CE contiene una especial protección de las comunicaciones únicamente serán válidas todas aquellas que se realicen mediante la resolución judicial motivada.

Por último, es de aplicación a cualquier derecho fundamental que se limite que la resolución judicial que lo determine se adapte al art. 141 LECrim que establece que será obligatorio que aquélla que dicte una limitación o merme un derecho fundamental deberá adoptar la forma de auto y con la motivación suficiente.

3.3. LA APORTACIÓN DEL CORREO ELECTRÓNICO AL PROCESO JUDICIAL.

La aportación del correo electrónico como prueba tecnológica en el proceso judicial, se ha de dar en el momento procesal oportuno, y en el proceso penal esa introducción a la causa se da en la fase de instrucción. En determinadas ocasiones, el contenido de tal prueba y su introducción en el proceso puede conllevar a la intromisión o vulneración del derecho a la intimidad o al secreto de las comunicaciones y en este caso serán nulas ya que tienen la consideración de prueba ilícita y como consecuencia, no tendrá cabida en el proceso. Por ello, se entiende que cualquier prueba que se incorpore al proceso será lícita en cuanto al respeto de los derechos fundamentales ya que de lo contrario no será objeto de análisis ni de incorporación al proceso penal. En otras palabras, será licita si se incorpora al proceso por alguna de las partes que haya sido partícipe de la conversación, si son aportados por un tercero, siempre y cuando, se dé el consentimiento de alguna de las partes y los que hayan sido obtenidos a través de una diligencia de investigación tecnológica en la que ha de ser preceptiva la autorización judicial correspondiente motivada de acuerdo con los principios regulados legalmente.[51]

Cualquier tipo de prueba electrónica que trate de incorporarse en el proceso penal, ha de garantizar la integridad y autenticidad de la misma, evitando de este modo, las impugnaciones que pudieran darse por la contraparte. Y, en especial consideración

[51]FUENTES SORIANO, O., "El valor…" Op. Cit., p.11.

del correo electrónico, que no basta con la mera transcripción de la conversación en papel o fotocopia de la misma que adquiere la consideración de prueba documental debido a que de esta forma su originalidad e integridad es prácticamente nula, y esto es debido, a la facilidad de que se producen alteraciones y modificaciones en relación con el documento original siendo inminente la impugnación de la misma por la contraparte. Si bien es cierto que, una forma de acrecentar la autenticidad sería la intervención de un fedatario público o de un notario emitiendo una diligencia de constancia o acta notarial respectivamente, pero la interpretación hecha por ambos se caracteriza por la ausencia de conocimientos informáticos, siendo su función la destinada a observar si el documento impreso se corresponde con el contenido del correo electrónico en el soporte digital. [52]

Por tanto, la única forma que entendemos para asegurar el valor probatorio del correo electrónico en el proceso judicial, es a través de la prueba pericial informática. Como consecuencia de la dificultad que se da para garantizar la fehaciencia del correo asímismo lo dispone FUENTES SORIANO[53] "debido al modo en que se estructura la información de un correo electrónico, solo mediante la práctica sobre el mismo de una prueba pericial informática se pondrán obtener datos concluyentes sobre su originalidad, veracidad e integridad." Aunque existe otro modo de garantizar la autenticidad e integridad de los correos electrónicos mediante las empresas que emiten certificados electrónicos en los que se certifica ello.

3.3.1. La prueba pericial informática.

En toda pericial informática es necesario establecer una cadena de custodia de las fuentes de información a analizar. En el caso concreto sería: del propio correo electrónico, archivo contenedor de correos electrónicos, etc. De este modo, se asegura el derecho a la defensa de la otra parte ya que permite a terceros verificar los resultados. La cadena de custodia se realiza mediante copia y depósito de la información ante Notario.

[52] MARTÍNEZ DE CARVAJAL HEDRICH, E. "Valor probatorio de un correo electrónico", Diario La Ley, nº8014,1 de febrero de 2013, año XXXIV, Editorial La Ley. p.1.
[53]FUENTES SORIANO, O., "El valor…" Op. Cit,, p.14.

En primer lugar, cabe por destacar la importancia de la elección del perito que ha de ser aquel tercero ajeno al proceso para garantizar la imparcialidad y objetividad del sujeto, y a su vez, que esté en posesión de unos conocimientos especiales de los cuales carezca el Juez enjuiciador y que son necesarios para asegurar la integridad de la prueba en cuestión. De modo que, entendemos por perito óptimo, todo aquel que esté en posesión de un título de licenciado en informática o sea ingeniero informático. [54] De no realizarse de esta forma, la pericia carecerá de reconocimiento judicial como medio probatorio.

En segundo lugar, la estructura del correo electrónico se divide en dos partes: la cabecera y cuerpo del mensaje.

La cabecera del correo electrónico es primordial para el análisis forense de la prueba pericial ya que en la misma hallamos toda la información caracterizadora de la comunicación que nos permite verificar la veracidad e integridad del documento en el que se plasma el correo electrónico aportado al proceso judicial. Por tanto, la cabecera comprende datos que nos proporcionan información relativa a la fecha y hora de emisión y recepción real del contenido de mensaje, del emisor y el receptor o destinatario, con independencia de la que tengan, tanto el emisor como el receptor del mensaje, en el dispositivo que se encuentre el correo. [55]

El perito informático que acceda al equipo en el que se encuentre el correo electrónico en el que se efectúa el análisis forense nos permite disponer de la siguiente información: quiénes son los sujetos que participan en el proceso de información (el remitente y el destinatario), cuándo se produce la redacción del mensaje, es decir, en qué fecha y hora, y cuándo se entrega o transmite el mensaje desde el proveedor del correo electrónico a la cuenta del destinatario. Asimismo, se procede a examinar distintas secciones como es la dirección de correo electrónico del destinatario y remitente, la fecha en la que llegó el mensaje a los servidores del correo, un número exclusivo designado por el proveedor del correo para indicar el mensaje, de dónde

[54] PUJOL CAPILLA P., *La nueva..." Op. Cit.*, p.23: "(…) en España, no existen titulaciones específicas en materia de tecnología forense o seguridad informática."
[55] FUENTES SORIANO, O., "El valor…" Op. Cit., pp.16-19.

proviene el correo y el recived[56], medio utilizado, la fecha, el remitente, el asunto y el destino, la información al redactar el mensaje. A su vez, cuando se procede al análisis del registro de los servidores que contienen información, hallamos las direcciones IP que identifican la huella cronológica o real del correo electrónico.

En relación con el contenido del mensaje del correo electrónico, es necesario resaltar que si garantiza la certeza del correo electrónico una vez finalizado el análisis de la cabecera del mensaje se está demostrando de manera prácticamente automática la veracidad del contenido del mismo. [57]

Una vez concluso la prueba pericial informática, se procede a la escritura del informe pericial por parte del perito especializado en la cuestión en el cual incluirá todos los datos que sean relevantes para la cuestión que es objeto de análisis. Ha de cumplir con todos requisitos que se disponen en el art. 335 LEC tales como que estén en posesión de conocimientos técnicos y prácticos que sean precisos para determinar la autenticidad y veracidad de la prueba, que el perito sea designado por el Tribunal y que sea sometido a juramento en el que manifieste que va a decir la verdad, entre otros. Cumplidos éstos, se procederá a su valoración judicial según las reglas de la sana crítica.

3.3.2. Los certificados electrónicos como garantía de autenticidad e integridad.

Existe otro modo de mostrar la autenticidad y veracidad de los correos electrónicos aportados al proceso, sin necesidad de acudir a la práctica de una prueba pericial informática, puesto que existen terceros de confianza llamados entidades o empresas de certificación electrónica o digital[58]. Entendiendo por certificado electrónico como dispone el artículo 6 de la Ley de Firma Electrónica: "es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos

[56]FUENTES SORIANO, O., "El valor..." Op. Cit., pp.18-19. "los datos más relevantes para determinar la autenticidad del correo son los que ofrecen el "Recived" estos aparatos identifican la ruta de los servidores por los que ha pasado el mensaje hasta llegar a su destinatario."

[57] MARTÍNEZ DE CARVAJAL HEDRICH, E., "Valor…" Op. Cit., p.55.

[58] Existen varias empresas de certificación electrónica, tales como Agencia Notarial de Certificación (ANCERT).

de verificación de firma a un firmante y confirma su identidad" todo documento electrónico que sea emitido por un tercero de confianza, que suele ser una autoridad de certificación, que garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública[59]. Tienen la finalidad de garantizar la autenticidad y veracidad de la información contenida en el correo a través de la firma electrónica la cual asegura la identificar al firmante y asegurar la integridad del documento firmado, lo que se traduce en que, el documento firmado es exactamente igual al original. Estos documentos electrónicos son expedidos por una autoridad de certificación e identifica a una persona que puede ser tanto física como jurídica. La finalidad de estos certificados es validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta. A su vez, abarca toda la información que se requiere para firmar electrónicamente e identificar a su propietario con sus datos tal como nombre, NIF, algoritmo y claves de firmas, fechas de expiración y organismo que lo expide. Con respecto a su funcionamiento, la Autoridad de Certificación se encarga de dar fe de que la firma electrónica se corresponde con un usuario concreto, y como consecuencia de ello, los certificados están firmados, a su vez, por la Autoridad de Certificación. Esto se trata, en definitiva, de una mayor fiabilidad antes de que se han entregados al interesado.[60]

Gracias a las empresas que se dedican a la emisión de certificados electrónicos y brindan de mecanismos de verificación de los documentos electrónicos y que sean introducidas con plenas garantías, suprimiendo así, prácticamente la posibilidad de que las pruebas electrónicas sean impugnadas en juicio.

Asimismo, el artículo 162 de la Ley de Enjuiciamiento Civil, permite la aportación de los documentos electrónicos certificados en juicio para su posterior valoración y así lo dispone el precepto "cuando las partes o los destinatarios de los actos de comunicación dispusieren de medios electrónicos telemáticos (…) que permitan el envío y la recepción de escritos y documentos, de forma tal que esté garantizada la autenticidad (…) los actos de comunicación podrán efectuarse por aquellos medios, con el resguardo acreditativo de su recepción que procede". Y así lo reconoce jurisprudencia del Tribunal Supremo reconoce mediante resolución judicial el valor probatorio del

[60] http://firmaelectronica.gob.es/Home/Empresas/Certificados-Electronicos.html(consultada el 25 de abril de 2016)

correo electrónico por parte de una empresa prestadora de servicios de comunicación hace constar que se ha producido la emisión, la recepción y hora (tanto de emisión como de recepción) del mensaje, es decir, la totalidad y veracidad del mismo, asegurando de este modo la no manipulación del mismo y su originalidad.[61]

Observamos que tienen la misma finalidad que una pericial pero con un proceso, a mi modo de ver, menos complejo y más rápido.

3.4. LA INTERVENCIÓN DEL CORREO ELECTRÓNICO COMO ACTO DE INVESTIGACIÓN JURISDICCIONAL.

Cada vez con más frecuencia, al ser el correo electrónico el medio telemático más utilizado por la sociedad de la comunicación, que los mismos sean relevantes en el seno de la investigación penal como fuente de información para clarificar los hechos delictivos que se le imputan a la persona que se le atribuye el término, recientemente novedoso, de investigado[62]. Y así lo establece nuestra legislación procesal penal, tras la inminente reforma efectuada por la LO 13/2015, gracias a la cual se cumple con el principio de reserva legal en materia de derechos fundamentales tal y como vemos en diversas sentencias del Tribunal Constitucional "por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE) o limite o condicione su ejercicio (art. 53.1 CE) efectivo, precisa una habilitación legal."[63]Una reserva de ley que constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas.

El artículo 579 de la LECrim bajo la rúbrica de "La detención y apertura de correspondencia escrita y telegráfica" se actualiza a los tiempos que corren en el que se

[61]Véase en el Auto de la Sala Primera del Tribunal Supremo 855/2010.
[62]Este término permite salvaguardar de mejor modo el principio de presunción de inocencia de la persona que se encuentra en tal situación.
http://noticias.juridicas.com/actualidad/noticias/10551-contenido-y-novedades-de-la-reforma-de-la-lecrim-por-la-ley-organica-13-2015-y-por-la-ley-41-2015/ (consultada el 13 de abril)
[63]Véase en la STS 49/1999, de 5 de abril.

modifica su ámbito material de aplicación, los plazos máximos de duración y la necesidad de una autorización judicial para que estas medidas de investigación, que a su vez, son limitativas a los derechos fundamentales del artículo 18 de nuestra Constitución, y en el caso concreto del correo electrónico, entendido según el artículo 2 d) de la Directiva 58/2002/CE, como "cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponibles para el público". Como dispone MARCHENA GÓMEZ[64] "en una primera aproximación, pues la intervención de las comunicaciones telemáticas mediante correo electrónico, en la medida en que representan una limitación del derecho constitucional al secreto de las comunicaciones (…)." A pesar, de a simple vista por su concepción del correo electrónico sólo limita el artículo 18.3 CE, esto no es del todo correcto, ya que encontramos numerosa doctrina constitucional relativa a la limitación de los derechos fundamentales del artículo 18 CE y asimismo establece que la protección del derecho al secreto de las comunicaciones alcanza solo el proceso de la comunicación pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos[65]. Admitiendo en cierto modo que, depende de cómo se intercepte el mensaje, ya sea una vez enviado y recibido, leído o no leído o que se encuentre en el proceso de comunicación mismo, se vulnerara un derecho u otro. Del mismo modo, se complementa con la incorporación del Título VIII del Libro II, en particular, los Capítulos V a VII en los que disponen el resto de medidas de investigación tecnológica.

Procediendo a analizar detalladamente el artículo 579 LECrim que faculta la intervención de la interceptación de la correspondencia:

"1. El Juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:

[64]MARCHENA GÓMEZ, M., "Dimensión jurídico-penal del correo electrónico" Diario La Ley, núm. 6475, Sección Doctrina, 4 May. 2006, Ref. D-114, Editorial La LEY, pp.23-27.
[65]Véase en la STC 123/2002, de 20 de mayo, a título de ejemplo.

1. º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2. º Delitos cometidos en el seno de un grupo u organización criminal.

3. º Delitos de terrorismo.

2. El Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses, la observación de las comunicaciones postales y telegráficas del investigado, así como de las comunicaciones de las que se sirva para la realización de sus fines delictivos.

3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

4. No se requerirá autorización judicial en los siguientes casos:

a) Envíos postales que, por sus propias características externas, no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías o en cuyo exterior se haga constar su contenido.

b) Aquellas otras formas de envío de la correspondencia bajo el formato legal de comunicación abierta, en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección.

c) Cuando la inspección se lleve a cabo de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío.

5. La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.”

Extractando del mismo, que como regla general para la interceptación de las comunicaciones postales que tienen el mismo tratamiento que el correo electrónico ha de ser preceptiva la autorización judicial

De acuerdo con la legislación vigente, para adoptar una medida de investigación tecnológica ya sea de intervención o de registros de comunicaciones es necesaria la autorización judicial adoptándola de acuerdo con los principios de excepcionalidad, especialidad, idoneidad, necesidad y proporcionalidad de la medida que se adopte que ha sido objetode tratamiento en la jurisprudencia del Tribunal Constitucional. A su vez, en el caso de las comunicaciones telemáticas postales, en la que se incluye el correo electrónico, será preceptiva para los delitos tasados en tal precepto. Se incluyen algunas excepciones cuando concurra razones de urgencia y se trate de delitos relacionados con bandas armadas o terroristas podrá dictar la resolución que habilite la interceptación y detención de la correspondencia, el Ministro del Interior y en su defecto, el Secretario de Estado de Seguridad, la misma será válida, siempre y cuando, pasadas veinticuatro horas, lo ratifique el Juez correspondiente. E, incluso, el precepto habilita la posibilidad de que en ciertos casos no sea necesaria la resolución judicial estando los mismos tasados en una lista cerrada.

4. LAS APLICACIONES DE MENSAJERÍA INSTANTÁNEA COMO MEDIO DE PRUEBA EN EL PROCEDIMIENTO JUDICIAL.

4.1 LA IRRUPCIÓN DEL *WHATSAPP* COMO MEDIO DE PRUEBA.

4.1.1 Consideraciones generales.

Como consecuencia del gran impacto tecnológico que sufre la sociedad actual se ha producido un cambio en el mundo de la comunicación haciendo un uso globalizado de Internet, dejando así de lado, las comunicaciones tradicionales tales como el correo postal e incluso disminuyendo las llamadas efectuadas y el envío y recepción de los

SMS a través del teléfono móvil siendo sustituidas por otras formas de comunicación que permiten los mismos teléfonos móviles, *tablets* y ordenadores. A causa de la masiva utilización de Internet en estos aparatos electrónicos que han impulsado la aparición de aplicaciones de mensajería instantánea, [66] como sustitutas de otras formas de comunicación debido a sus grandes ventajas, ya que permiten una comunicación a tiempo real entre dos o más personas. Su gran uso no puede dejar inadvertido al ámbito de lo jurídico, y es que cada vez, es más frecuente la presentación de mensajes y conversaciones que tienen lugar a través de las aplicaciones de mensajería instantánea en los procesos judiciales.

Hoy en día contamos con diversas aplicaciones de mensajería instantánea tales como *Telegram, Line, WeChat* entre otras, pero sin lugar a dudas, la aplicación más conocida y que más usuarios ha captado, con más de 600 millones en todo el mundo, es *WhatsApp.*[67]

El *WhatsApp* permite el intercambio de mensajes de texto ilimitados, imágenes, vídeos, notas de audio, compartir contactos e incluso la ubicación, entre los contactos que se encuentren en la agenda de teléfono del usuario, siempre y cuando, esos contactos dispongan de la aplicación en los respectivos dispositivos electrónicos ya sea el *Smartphone, Tablet* u ordenador. A su vez, se caracteriza por la necesidad de una tarifa de datos 3G o por conexión *Wifi* y ser gratuita. Se encuentra disponible en multiplataforma: *IOS, Android, Windows Phone, BlackBerry Os.* Con respecto a su funcionamiento, es diferente al de las redes sociales o blogs debido a que en éstos la

[66] IM son las siglas en inglés de *instant messaging* (mensajería instantánea) y es un servicio de comunicación de tiempo real entre dispositivos como computadoras, tabletas, celulares, etc. La mensajería instantánea se basa en el uso de programas conocidos como clientes de IM (*IM clients*, en inglés) que se instalan en una computadora o dispositivo móvil. Para que dos personas se puedan comunicar usando IM, cada uno debe tener instalado uno de estos programas, que se conectan entre sí para enviar mutuamente mensajes de texto e imágenes pequeñas.
http://aprenderinternet.about.com/od/ChatsForosEtc/a/Que-Es-Im-O-Mensajeria-Instantanea-Y-Como-Funciona.htm (consultada el 18 de mayo de 2016)

[67] Véase en "Las mejores aplicaciones de mensajería instantánea publicado" en el diario ABC, el día 11 de noviembre de 2014.
http://www.abc.es/tecnologia/top/20141111/abci-whastapp-aplicaciones-mensajeria-instantanea-google-hangouts-wechat-line-telegram-facebook-messenger-spotbros-201411111226_1.html (consultada el 20 de mayo de 2016)

información que se transfiere o comunica permanece almacenada durante un periodo de tiempo en las sabes de datos del administrador. [68]

Una de sus características más destacables, trata de que la información enviada y recibida entre los usuarios no es conservada por un tercero o servidor externo a los dispositivos o soportes electrónicos a través de los que se genera o produce la comunicación perteneciente al administrador, de este modo, solo se conserva en el soporte de los comunicantes. Con respecto a ello, alude RODRIGUEZ LAINZ[69] que el administrador de la aplicación de *WhatsApp* únicamente proporciona el tránsito de la información entre los comunicantes y, a su vez, otorga protocolos de seguridad para garantizar el cifrado de la información.

Por otro lado, no hay que olvidar que como todas las comunicaciones electrónicas no generan dificultad de manipulación lo que cuestiona su integridad y autenticidad y, es más, dicha característica particular agrava más la cuestión de autenticidad, validez y eficacia de este soporte como prueba en un procedimiento judicial.

4.1.2. Como medio de prueba.

En primer lugar, hay que entender que proponer un mensaje de *WhatsApp* como medio de prueba o de cualquier otra aplicación de mensajería instantánea es equiparable a la proposición de como medio de prueba de cualquier otra comunicación que haya tenido lugar a través de un dispositivo o medio electrónico.[70]

---

[68]DELGADO MARTÍN, J., "La prueba de WhatsApp" Diario La Ley, Nº8605, Sección Tribuna, Ref. D-331, Editorial La Ley, p.1.

[69]RODRIGUEZ LAINZ, J. L., "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea*"* Diario La Ley, núm 8569, Sección Doctrina, 25 de junio de 2015, p.4.

[70] MARTUS BACARIA, J., "El caso WhatsApp. Las aplicaciones de mensajería instantánea como medio de prueba en el procedimiento judicial.", Economist&Jurist. p.81 http://www.economistjurist.es/articulo-derecho-civil-penal-mercantil-laboral-fiscal-procesal-publico-privado-administrativo-internacional/el-caso-whatsapp-las-aplicaciones-de-mensajeria-instantanea-como-medio-de-prueba-en-el-procedimiento-judicial/ (consultada el 17 de mayo de 2016)

En segundo lugar, cabe por destacar que en relación con la aceptación de las aplicaciones de mensajería instantánea como medio de prueba, la Ley de Enjuiciamiento Criminal no recoge en su articulado ningún precepto en el que se regulen estos medios de prueba plasmados en soportes telemáticos, acudiendo como consecuencia de ello, de forma subsidiara, a la Ley de Enjuiciamiento Civil, en particular, al precepto 299.2: *"*También, se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.*"*A su vez, les será de aplicación los artículos 382 a 384 de la misma Ley. Entendiendo así que estas aplicaciones de mensajería instantánea instaladas en el respectivo soporte electrónico, son aceptadas como medio de prueba para ser aportados en juicio. Asimismo, hay que considerar que el art. 299.1 se regulan los medios de prueba tradicionales, así pues, estas aplicaciones pueden introducirse al proceso, además, adoptando las características de estos medios de prueba talescomo prueba documental, sea pública o privada, la prueba pericial, a través del reconocimiento judicial o mediante el interrogatorio de partes o testigos como prueba personal.

Por tanto, todos los medios de prueba previstos por la Ley, son adecuados para incorporar en el procedimiento penal que corresponda, los datos e información contenida en los sistemas de mensajería instantánea. Ahora bien, incluso, es recomendable, que se sirvan de distintos medios de prueba aceptados por el ordenamiento jurídico, para otorgar mayor seguridad de la autenticidad e integridad, tratando así de eliminar cualquier sospecha de manipulación.

El medio de prueba más adecuado para la introducción de datos o información mantenidos a través de aplicaciones de mensajería instantánea, consiste en la entrega del soporte electrónico en el que ha tenido lugar la comunicación unido a una transcripción de los mensajes como bien dispone el art. 382.1 LEC al permitir a las partes que propongan los propios soportes telemáticos como medio de prueba, siempre y cuando, se acompañen de la transcripción escrita de las palabras contenidas en los mismos, en tales casos, los *Smartphones*, y han de ser relevantes para el proceso. A su vez, para garantizar su autenticidad y veracidad han de ser cotejados por el Letrado de la

Administración de Justicia para que establezca diligencia de constancia de los mismos[71] o por el Notario que levante acta notarial en la que haga referencia que la transcripción no ha sufrido alteración con respecto a la que se encuentra en el dispositivo. También puede darse como prueba de su integridad que, en ciertas ocasiones, se muestre el dispositivo del otro comunicante para asegurar así la veracidad de los mismos pero, rara vez, ocurre en la práctica.

Así pues, en tales casos, la prueba aportada sería válida a la expensa de la valoración judicial en la que será más que relevante la impugnación o no de la parte contraria. Pudiendo darse dos situaciones: 1) que la contraparte alegue la impugnación de esa prueba de forma motivada o 2) que la contraparte no impugne la autenticidad e integridad de la prueba[72]. Sin embargo, en la práctica, es muy difícil que no se produzca tal impugnación por parte de la contraparte, no obstante, en el caso de que no se dé el Juez habrá de tenerla como auténtica y exacta, siendo así que la será valorada en relación con el resto de pruebas aportadas al proceso y que han sido válidas también.[73]

Pero si se procede tal impugnación por la parte contraria, como es lo habitual, en la que se suele alegar la manipulación o falsedad de la prueba, el Juez la valorará conforme a las reglas de la sana crítica y, a continuación, como alude DELGADO MARTÍN[74] el Juez o Tribunal procederá a valorar los siguientes elementos: el propio contenido de los motivos de impugnación alegados por la parte contraria, los otros medios probatorios relativos a los concretos mensajes que pretenden ser probados como son las declaraciones de los acusados o interrogatorio de partes y las declaraciones testificales que garanticen la integridad y exactitud de la prueba. En tal caso, la carga de la prueba, recae sobre la parte que se beneficie de la validez del medio probatorio impugnado, quién deberá aportar la realización de una prueba pericial al proceso mediante la que se garantice la fehaciencia del contenido de los mensajes en la que tendrá tratamiento de análisis del dispositivo electrónico para que se efectúe examen.

[71]Véase en la Sentencia de la Audiencia Provincial de Córdoba SAP CO 324/2014 número de la resolución 159/2014, de 2 de abril.
[72] Véase en la SAP CO 324/2014, a título de ejemplo.
[73]DELGADO MARTÍN, J., "La prueba…" Op. Cit., p.4.
[74] DELGADO MARTÍN, J., "La prueba…" Op. Cit., pp. 4 y 5.

Con respecto al índice temporal del proceso en el que se aportan los medios probatorios, han de ser introducidos en el momento procesal oportuno, y en el caso del proceso penal, se trata de la fase de instrucción. Sin olvidar, que las fuentes de prueba que se pretendan hacer valer en juicio han de introducirse en cualquier soporte que sea objeto de reproducción en el juicio oral.

A partir de su introducción en el proceso, es conveniente con la finalidad de garantizar la integridad y autenticidad de la prueba presentada, así como para eliminar toda oportunidad de manipulación que pueda haber o darse, que se dé o se haga llamamiento a la preservación de la cadena de custodia tanto, en el momento de la obtención como, en el de conservación de la prueba.

Ahora bien, es de aplicación general que, cualquier medio de prueba que se proponga o se aporte ha de ser obtenido de manera lícita, ha de cumplir con el presupuesto de la licitud probatoria, en otras palabras, que no haya vulnerado o violado ningún derecho fundamental y, en el caso de las comunicaciones electrónicas, los derechos fundamentales contenidos en el artículo 18 CE, en particular, el derecho al secreto de las comunicaciones y el derecho a la intimidad. De lo contrario, será de aplicación el artículo 11.1 de la LOPJ: "no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales" estaríamos hablando en este caso de una prueba prohibida que tiene vedado el acceso al procedimiento. De acuerdo con lo anterior, cabe hacer referencia al art. 287 LEC que establece cómo se determinará la ilicitud de la prueba.

En relación a los derechos fundamentales que pueden resultar vulnerados con la aportación al proceso de un medio de prueba de estas características, es decir, de contenidos de conversaciones transcurridas a través de los soportes de mensajería instantánea, surten de un lado, el derecho a la intimidad que se entenderá lesionado cuando no se respete el artículo 7 de la LO 1/1982, de 5 de mayo, sobre protección civil del derecho a la intimidad personal y familiar y a la propia imagen que recoge que se entiende por intromisiones no permitidas en la intimidad y el artículo 197 del Código Penal. Y, de otro lado, el derecho al secreto de las comunicaciones que comparte ámbito de protección en el artículo 197 CP, aunque tienen una protección diferente estos

derechos a salvedad de este precepto. En tal caso las comunicaciones habrán de estar protegidas con independencia del contenido de la misma.[75]

Y, por último, en cuanto a la valoración judicial de este tipo de prueba electrónica, únicamente habrán de valorarse aquella que cumpla con los requisitos de incorporación al proceso como son el de pertenencia, necesidad y licitud de la prueba. A su vez, el Juez le atribuirá mayor o menor fuerza probatoria a aquellas que sean más determinantes para clarificar el hecho objeto de enjuiciamiento. Así como, toda decisión que adopte el Juez con respecto a la prueba en cuestión ha de estar debidamente motivada en la resolución judicial que se dicte.[76]

4.2. LOS POSIBLES RIESGOS DE MANIPULACIÓN EN LAS APLICACIONES DE MENSAJERÍA INSTANTÁNEA COMO MEDIO DE PRUEBA.

Como todo soporte electrónico conectado a una red de Internet, ya sea por cable o inalámbrica, el uso de las aplicaciones de mensajería instantánea posee ciertos riesgos a causa de la enorme facilidad con la que se puede usurpar la identidad de un usuario haciéndose pasar otra persona por el usuario emisor o receptor, crear conversaciones ficticias o borrar determinados mensajes enviados y recibidos entre los comunicantes simulando así una conversación distinta a la original. A su vez, también puede darse que se produzca tanto la pérdida como la sustracción del aparato, entre otros muchos más. Así pues, lo refleja reciente jurisprudencia del TS en la que se dispone que "la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo[77]."

A parte de los riesgos propios que cualquier dispositivo electrónico posee, las aplicaciones de mensajería instantánea se encuentran con un obstáculo añadido, se trata

[75]MARTUS BACARIA, J., "El caso…" Op. Cit., pp. 82 y 83.
[76]DELGADO MARTÍN, J., "La prueba…" Op. Cit., pp. 5 y 6.
[77] Véase en la STS 300/2015.

de la particularidad de su funcionamiento y es que el propio administrador de la empresa *WhatsApp Inc.*, no guarda ni conserva las conversaciones mantenidas por sus usuarios a través del uso de su aplicación, es decir, ningún servidor externo a la comunicación que no sean los comunicantes conoce la conversación mantenida, lo que significa, que fácilmente podrán eliminar partes de la misma sin que nadie pueda desmentirlo a priori[78]. Por ello, es interesante resaltar, como dispone BELTRÁN PARDO[79] que "la única forma de acreditar la existencia de estos contenidos es a través de los teléfonos móviles que han intervenido como emisor y receptor. No se guardan, pues, en la tarjeta SIM, sino en memoria interna del aparato o en la tarjeta de memoria tipo SD, la cual, si es trasladada a otro terminal no puede recuperar la información que haya sido borrada intencionadamente por el usuario."

Existen diversos modos de proceder a manipular las conversaciones de las aplicaciones de mensajería instantánea, ya sea desde niveles básicos como expertos, de tal forma que se puede llegar incluso a no dejar rastro de los mensajes enviados y recibido y que un análisis pericial pase inadvertido estos mensajes. Se puede crear una conversación plenamente ficticia a través de la base de datos idéntica a la original. [80]

Así como, título de ejemplo en el diario el Mundo, en su edición digital de 1 de octubre de 2015 se explica cómo es posible la manipulación siguiendo los siguientes pasos: "en primer lugar, la base de datos de *Whatsapp* está cifrada en criptografía simétrica. Lo que quiere decir que se utiliza la misma clave para cifrar y para descifrar la base de datos que está almacenada (y de fácil acceso) en el directorio que utiliza *Whatsapp*. Sin embargo, la base de datos original (la que se utiliza para guardar los

[78]BELTRÁN PARDO, A. I., "Los contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo". Noticias jurídicas, p.4.
http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533-las-contenidos-de-whatsapp-como-medio-probatorio-en-el-ambito-de-las-diligencias-urgentes-por-delitos-de-violencia-contra-la-mujer-cuestiones-en-torno-a-su-impugnacion-y-a-la-practica-de-la-prueba-pericial-a-la-que-se-refiere-la-sts-300-2015-de-19-de-mayo/
(consultada el 10 de mayo de 2016)
[79]BELTRÁN PARDO, A. I., "Los contenidos…" Op. Cit., p.4.
[80]Véase en "Los mensajes de WhatsApp se pueden manipular sin dejar rastro", Diario el Mundo, edición digital, del 1 de octubre de 2015.
http://www.elmundo.es/tecnologia/2015/10/01/560d531a22601d40448b459b.html
(consultada el 25 de mayo de 2016)

mensajes después de ser enviados o recibidos), no está cifrada, sino que se encuentra en uno de los directorios que la aplicación tiene en el sistema operativo. Para acceder a esta base de datos, el móvil en cuestión tiene que ser configurado en modo 'súper-usuario' o privilegiado, para así tener acceso a todas las funciones del terminal, algo relativamente sencillo incluso para usuarios no expertos (existen varias aplicaciones, tutoriales y explicaciones disponibles en la web para ello). Cuando ya tenemos acceso a la base de datos original, se ejecutan una serie de comandos para acceder a la base de datos de *Whatsapp*. Luego hay que moverse en el directorio hasta identificar el fichero que se quiere manipular. Después se ejecutará otro comando para llevar a *Windows l*a base de datos (previamente habrá que haber realizado una copia de seguridad de los mensajes desde la aplicación *Whatsapp*). Con el programa adecuado, esa base de datos se abre en *Windows.* Después se navegará hasta las tablas llamadas *'messages'* que almacenan los mensajes y finalmente se editará el texto de esos mensajes. El proceso completo está pueden manipular mensajes enviados y recibidos, también es posible generar mensajes que no existían, aparentemente procedentes de cualquier teléfono del mundo, incluso de números inexistentes."[81]

A causa de las grandes vulnerabilidades que desprenden las aplicaciones de mensajería instantánea para que sean aceptadas como prueba electrónica íntegra y auténtica, cabe por destacar que este tipo de pruebas como son las derivadas de los sistemas de mensajería instantánea han de ser abordadas con todas las cautela, lo que quiere decir, que han de someterse a un examen pericial informático exhaustivo que tendrá una gran complejidad, como consecuencia de que para eliminar toda posibilidad de manipulación no es suficiente con una copia de la conversación en papel y entrega del dispositivo que se encuentra junto con el cotejo del mismo por parte del Letrado de la Administración de Justicia o del Notario que levante acta notarial.

[81]Véase en "Los mensajes…" Op. Cit.

4.3. LA PRUEBA PERICIAL INFORMÁTICA EN LAS APLICACIONES DE MENSAJERIA INSTANTÁNEA.

Considerando que la aplicación de *WhatsApp*, como cualquier otro sistema de mensajería instantánea, es sencillamente vulnerable a la vez que manipulable, la jurisprudencia del TS[82] establece que "la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas." Por tanto, se entiende que éstas deben ir acompañadas del soporte electrónico dónde tuvo lugar la conversación, de la transcripción de la misma, junto con un análisis pericial informático como así se dispone que: "será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido."

El objetivo primordial de realizar la prueba pericial informática es demostrar la ausencia de manipulación o falsificación de los mensajes tanto enviados como recibidos. Si bien es cierto, el único modo de autentificar los mensajes contenidos en tales soportes es mediante la realización de un análisis forense informático.

Una de las características para poder efectuar la prueba pericial informática, a rasgos generales, es el necesario consentimiento de las partes, o en su defecto, de la autorización judicial correspondiente, de lo contrario, se devendrá como nula e ilícita ya que como consecuencia de ella se puede vulnerar los derechos fundamentales de las partes tales como los contenidos en el mencionado artículo 18 CE.[83]

Ante el tipo de prueba electrónica de aplicaciones de mensajería instantánea, en concreto, la de *WhatsApp*, presenta una dificultad añadida como consecuencia de que el administrador de la empresa *WhatsApp Inc.*, no recopila el contenido de las conversaciones mantenidas por sus usuarios a través de la aplicación, quedando éstas solamente conservadas en los dispositivos del emisor y receptor de la comunicación. Y, por tanto, en aquellos casos de que se borren por parte de los usuarios los mensajes que fueron enviados y recibidos complican el examen pericial a realizar. Asimismo, alude

[82]Véase en la STS 300/2015.
[83]BELTRÁN PARDO, A. I., "Los contenidos…" Op. Cit., pp.11-13.

BELTRÁN PARDO[84] que "la única información que pueden facilitar es la que se denomina metadatos, que pueden ser definidos como datos sobre datos o la información generada por los usuarios cuando utilizan tecnologías digitales. Tienen la consideración de metadatos, la constatación del tráfico de las comunicaciones, origen y destino de las mismas, datos conservados sobre identidades y nombres de usuario y claves, incluidos el número de abonado telefónico asociado o la IP de referencia. No obstante, todos los datos de tráfico de esta aplicación, incluidas las conversaciones futuras, pueden ser objeto de interceptación a través de la correspondiente autorización judicial, pero el acceso a contenidos ya emitidos no resulta posible si se acude al administrador de la aplicación." Así pues, dada la dificultad que supone la realización de una pericia informática de tal calibre solamente podrá ser confeccionada por peritos que se encuentren en posesión de un título de ingeniero informático y que se encuentre colegiado.

Ahora bien, la práctica de una prueba pericial informática de este calibre tiene por objeto analizar de manera exhaustiva la memoria interna del dispositivo electrónico, que en el caso de *WhatsApp* suele ser el *Smartphone*, que pertenezca tanto al emisor como al receptor ya que se trata de la única forma de garantizar la fehaciencia de las comunicaciones mantenidas entre ambos y la falta de manipulación de la misma. Asimismo, la puesta en práctica de la misma se efectúa el examen forense íntegro y profundo de todos los elementos que sean claves y primordiales para decretar la autenticidad e integridad de las conversaciones tales como: el análisis de la memoria del dispositivo qué es objeto de examen, determinar los códigos propios del programa de mensajería en cuestión, en este caso del *WhatsApp*, los archivos temporales que surgen y se encuentran ocultos en tal dispositivo, entre otros, a título de ejemplo.

El examen pericial recae sobre el dispositivo de aquél a que le corresponde la carga de la prueba, dicho de otro modo, del que le favorece el reconocimiento de autenticidad e integridad dicha conversación o transcripción de mensajes para que la misma constituya prueba válida. Sin embargo, lo ideal sería que se realizará en ambos

[84]BELTRÁN PARDO, A. I., "Los contenidos…" Op. Cit, p.4.

dispositivos que han participado o han tomado parte de la comunicación bidireccional o multidireccional.

Por un lado, si se trata de demostrar la autenticidad de mensajes recibidos, el análisis se llevará a cabo en terminal receptor con la finalidad de determinar que desde ese mismo terminal no se produjo ningún tipo de manipulación en relación con en el contenido del mensaje. Y, de otro lado, si se trata de verificar los mensajes enviados sería conveniente revisar y analizar el terminal en este caso del emisor de la comunicación compartiendo en todo caso la misma finalidad.

Ahora bien, no hay que olvidar, que el perito informático puede ponerse en contacto con la empresa *WhatsApp Inc.*, de acuerdo con la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes de comunicaciones en el artículo 1:

"1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas".

Con la finalidad de que le facilite ciertos datos que sean indispensables para practicar la misma, aunque esa obligación de transmitir los datos se encuentra limitada por las particularidades de la aplicación.

Una vez realizado el informe pericial por un perito informático colegiado en el que quede acreditada la autenticidad e integridad, así como, descartada la manipulación de la conversación, la prueba devendrá válida y será objeto de valoración con las restantes pruebas presentadas y aceptadas en el procedimiento.

4.4. LA INFLUENCIA DE LA SENTENCIA DEL TRIBUNAL SUPREMO NÚMERO 300/2015, DE 19 DE MAYO, EN LAS APLICACIONES DE MENSAJERÍA INSTÁNTANEA.

Hace unos meses atrás el Tribunal Supremo dictó una sentencia, en concreto, el 19 de mayo de 2015, que ha sido de gran repercusión para la aceptación de pruebas electrónicas basadas en capturas de pantallas de conversaciones mantenidas a través de una red social, como es en el caso que ocupa a la sentencia en *Tuenti*, que, a su vez, es equiparable a todas aquellas mantenidas por aplicaciones o sistemas de mensajería instantánea.

Por un lado, esta sentencia muestra las grandes vulnerabilidades de los nuevos sistemas de comunicación surgidos a causa del gran impacto tecnológico globalizado, así como, dispone STS 300/2015, de 19 de mayo al establecer que "la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo.*"* Aquí refleja la gran fragilidad de estas pruebas al aportarlas al proceso ya que su grado de manipulación es muy elevado dado a la sencillez con la que pueden ser manipuladas.

Por otro lado, la misma refleja que las pruebas electrónicas han de ser obtenidas y presentadas con todas las cautelas, asimismo se dispone "la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas."

A causa de ello, para que otorguen completo y absoluto valor probatorio estaremos ante la obligación de efectuar la práctica de una prueba pericial como así se muestra: "será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.*"*

Y, respecto a la carga de la prueba, le corresponde siempre a la parte que la aporta al proceso, es decir, a aquella parte que se vaya a favorecer de la admisión de la prueba en juicio para demostrar el hecho que es objeto de enjuiciamiento. Asimismo "desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria."

Para concluir, podríamos decir que esta sentencia esclarece ciertos puntos sobre la admisión de este tipo de prueba estableciendo que al ser tan manipulables es siempre de obligado cumplimiento que se realicen todas las pruebas y medios pertinentes que estén al alcance de la parte que la propone para demostrar su veracidad e integridad.

5. CONCLUSIONES

1. A pesar de la reciente reforma producida por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, mediante la cual se producen novedades más que necesarias. Sin embargo, no se encuentra en tal texto normativo ninguna disposición en la que se regule cómo, cuándo y mediante qué medio probatorio han de aportarse las comunicaciones telemáticas como prueba de las nuevas tecnologías por las partes al proceso.
2. Ante la inexistencia de normativa o regulación específica de la prueba tecnológica, nos obliga a remitirnos a las reglas generales para la aportación y valoración judicial de la prueba introducida al proceso en cuestión. Dicho de otro modo, a las disposiciones comunes relativas a la prueba que se encuentran reguladas en la Ley de Enjuiciamiento Civil.
3. Nos encontramos ante una necesidad vigente de regulación específica de dicha prueba debido a las particularidades y peculiaridades que la caracterizan tales como, la sencillez con la que se vulneran los derechos fundamentales ya mencionados, la frecuente manipulación que se da en estas pruebas, así como las dificultades de reconocimiento por parte de la contraparte o del Juez correspondiente que conlleva la misma.
4. Como consecuencia de ello, nos vemos obligados a la hora de aportar una prueba cuyo contenido haya tenido lugar mediante un soporte digital de cumplir con todas las cautelas que estén al alcance de las partes con la finalidad de garantizar la integridad y veracidad de la prueba aportada, es decir, la ausencia de manipulación y falsificación de dicho medio probatorio.
5. Existen varias formas de garantizar y mostrar la autenticidad e integridad del documento electrónico que se pretende hacer valer como prueba al proceso, unas más fiables que otras, como son: la fe pública judicial o notarial, la práctica de una prueba pericial informática y un tercero ajeno al proceso que suele ser entidades o empresas que se encargan de expedir certificados electrónicos.
6. Con respecto a la fe pública judicial o notarial, se entiende como una forma de aumentar la fiabilidad de la prueba tecnológica aportada pero, es cierto que ésta carece de conocimientos específicos que requieren este tipo de pruebas que no

poseen ni el Letrado de la Administración de Justicia ni el Notario para certificar si verdaderamente no se ha producido la vulneración de los derechos fundamentales en su obtención, si no se trata de una información ficticia creada por la parte o un tercero beneficiado en la validez de la misma, o que haya sido manipulada por parte del usuario o de un tercero. Por ello, es frecuente que varios Letrados de la Administración de Justicia se nieguen a practicar el debido cotejo del dispositivo motivando su negativa en la ausencia de conocimientos para saber si es correcto o no lo que van a disponer en la diligencia.

7. La práctica de la prueba pericial informática supone un análisis íntegro del dispositivo electrónico en el que ha tenido lugar la conversación que es objeto de prueba en un proceso penal en cuestión. Con la finalidad de determinar si realmente es íntegra y auténtica o si, por el contrario, ha sido manipulada por uno de sus usuarios o por un tercero, o si ha sido creada ficticiamente para un beneficio plenamente ilícito. Dada la dificultad que supone es realizada por ingenieros informáticos que se encuentren debidamente colegiados. Solo mediante la misma, se pueden garantizar la fehaciencia y licitud de ese medio de prueba. Aunque si bien, a veces, ni un examen pericial puede garantizarlo puesto que si es manipulada por expertos puede llegar a pasar por inadvertido y esto puede ocurrir sobre todo en las aplicaciones de mensajería instantánea. A la vez, que cuentan con el inconveniente de que a instancia de parte suponen un elevado gasto económico por parte de aquél que pretende hacerse valer del medio probatorio.
8. Los certificados electrónicos como medio para garantizar la autenticidad e integridad de los dispositivos electrónicos son llevadas a cabo por un tercero, que suele ser una empresa, que se dedica a certificar la autenticidad de documentos electrónicos. Esto puede ser una gran alternativa a la práctica de la prueba pericial informática sobre todo en el caso de los correos electrónicos, cuyo funcionamiento es más sencillo y menos costoso económicamente.
9. Con motivo de los constantes avances de la sociedad de la información y la aparición de distintos tipos de prueba tecnológica al proceso nos encontramos ante una escasa jurisprudencia tanto a nivel nacional por parte del Tribunal Supremo y Tribunal Constitucional, así como a nivel internacional por parte del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos.

10. Por tanto, dada la ausencia de regulación específica respecto a su tratamiento y a la escasa jurisprudencia, nos vemos obligados a acudir a la regulación general de la prueba, así como a la jurisprudencia existente.
11. Por último, a día de hoy, nos encontramos con lagunas jurídicas respecto a estas pruebas dado a su carácter novedoso que aún están por resolver.

6. BIBLIOGRAFÍA

ÁLVAREZ CONDE, E., TUR AUSINA, R. *Derecho Constitucional*, Ed. Tecnos, Madrid, 5ª Edición, 2015.

ASENCIO MELLADO, J.M. *Derecho Procesal Penal*, Ed. Tirant lo Blanch, Valencia, 7ª Edición, 2015.

ASENCIO MELLADO, J.M. *Derecho Procesal Civil*, Ed. Tirant lo Blanch, Valencia, 2ª Edición, 2012.

BUENO DE MATA, F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", Diario LA LEY, Nº8627, Sección Doctrina, Ref. D-382, 19 de Octubre de 2015.

BUENO DE MATA, F., "La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica". Diario de la Ley, Nº8728, 23 de marzo de 2016, Ref. D-124, Editorial LA LEY.

CARRETERO SÁNCHEZ, S., "Las redes sociales y su impacto en el ataque a los derechos fundamentales: aproximación general". Diario La Ley, Nº8718, Sección Doctrina, 9 de marzo de 2016, Ref. D-99, Editorial LA LEY.

DELGADO MARTÍN, JOAQUÍN. "La prueba del *whatsapp*" Diario La Ley, núm. 8605, Sección Tribuna, 15 Sep.2015, Ref. D-331, Editorial LA LEY

DE QUINTO ZUMÁRRAGA, FRANCISCO. *Sabelotodo de Nuevas Tecnologías*. Barcelona. Ed. Difusión Jurídica 2004.

DE URBANO CASTRILLO, E., "La regulación legal de la prueba electrónica: una necesidad pendiente (1)", La Ley Penal, nº82, Mayo 2011, Editorial La Ley.

DOMINGO MONFORTE, J., "La intervención judicial de las comunicaciones". Actualidad Jurídica Aranzadi núm. 896/2014, Editorial Aranzadi, SA.

FUENTES SORIANO, O. (Coord.) "Comunicaciones telemáticas: práctica y valoración de la prueba.", *El proceso penal actual*, Tirant lo Blanch, Valencia, *en prensa*.

FUENTES SORIANO, O., "El valor probatorio de los correos electrónicos", en ASENCIO MELLADO (Coord.), *El proceso penal ante nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, *en prensa*.

FUENTES SORIANO, O., "La intervención de las comunicaciones tecnológicas tras la reforma de 2015*" en VVAA, Jornadas sobre la reforma de la Ley de Enjuiciamiento Criminal*. Primer Memorial Prof. Dr. Manuel Serra Domínguez, *en prensa.*

MARCHENA GÓMEZ, M., "Dimensión jurídico-penal del correo electrónico", Diario La Ley, núm. 6475, Sección Doctrina, 4 May. 2006, Ref. D-114, Editorial La LEY.

MARTÍNEZ DE CARVAJAL HEDRICH, E., "Valor probatorio de un correo electrónico", Diario La Ley, núm. 8014, Sección Práctica Forense, 1 Feb. 2013, Año XXXIV, Editorial La LEY.

MENÉNDEZ, L., "Nuevos tiempos, nuevas pruebas" en Escritura Pública, núm 83, Septiembre/ octubre 2013.

PASAMAR, A., "La prueba pericial informática frente a la impugnación de la autenticidad de un e-mail" ESADE, Barcelona, 8 de abril de 2011.

PORTAL MANRUBIA, J., "La regulación de la prueba electrónica en el proceso penal". Revista Aranzadi de Derecho y Proceso Penal núm. 31/201. Editorial Aranzadi, SA.

PUJOL CAPILLA, P., La *nueva prueba documental en la era digital. Su valoración en juicio*., Ed. Jurídica SEPÍN, Madrid, 2014.

RODRÍGUEZ LAINZ, JOSÉ LUIS., "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2. ª, 300/2015, 19 de mayo) (1)". Diario La Ley, Nº8569, Sección Doctrina, 25 de junio de 2015, Ref. D-256, Editorial LA LEY.

VELASCO NÚÑEZ, E., "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica". Diario La Ley, Nº 8183, Sección Doctrina, 4 de Noviembre de 2013, Editorial La LEY.