UNIVERSIDAD MIGUEL HERNÁNDEZ

FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE

GRADO EN DERECHO

LAS NUEVAS TECNOLOGÍAS COMO MEDIO DE PRUEBA EN EL PROCESO PENAL

TRABAJO DE FIN DE GRADO

CURSO 2015- 2016

Autor: Laura Quiles Mollá

Tutor: Pedro Vicente Martínez Cánovas

ÍNDICE

RESUMEN

El objeto del presente trabajo versa sobre el análisis de las nuevas tecnologías como medio de prueba, de cómo surgen y cuáles son las pruebas más comunes presentadas en juicio, cómo se obtienen, se aportan en el proceso penal y si en el momento de la obtención vulneran algún derecho fundamental recogido en el artículo 18 de la Constitución.

Asimismo, centrándonos en el correo electrónico como medio probatorio, cómo se ha de realizar su aportación, la práctica de la prueba pericial informática como medio de garantía de tal prueba, así como otros medios y la posibilidad de intervención del correo como diligencia de investigación tecnológica.

Y, en último lugar, *el WhatsApp* como medio de prueba, la facilidad de manipulación que se puede dar en estos casos y las características del examen pericial informático en tal aplicación.

ABSTRACT

The present report focuses on the analysis of the new technologies as a means of evidence, how arise and which the most common ones are presented at trial, how they are produced and used in the criminal process, and if they infringe the fundamental right that is laid down in the article 18 of the Constitution.

Furthermore, focusing on the electronic mail as value of evidence, how to make a contribution, the computer practical training as a means of guarantee such as other methods and the possibility of the intervention of the e-mail as a diligence of a technological research.

Finally, the *WhatsApp* shall be accepted as a means of evidence, the ease of handling that can be used in these situations and the characteristics of the expert computer exam of such an application.

ABREVIATURAS

AP	Audiencia Provincial
Art. /Arts.	Artículo/ Artículos
BOE	Boletín Oficial del Estado
CC	Código Civil
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
Coord.	Coordinador
CP	Código Penal
Dir.	Director
LEC	Ley de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal
LEF	Ley de Firma Electrónica
LN	Ley Notarial
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial
Núm.	Número
Op. Cit.	Obra Citada
SAP	Sentencia de la Audiencia Provincial
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y Comunicación
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
P.	Página
Pp.	Páginas
VVAA	Varios Autores

1. INTRODUCCIÓN.

En la sociedad actual se vive una inmensa masificación y expansión de las tecnologías de la información y comunicación. Nos encontramos ante un uso de estas nuevas tecnologías totalmente globalizado por parte de cualquier persona con independencia de la edad, de las preferencias, del lugar, entre otras. Desde su aparición por primera vez a mediados del siglo XX han ido calando en cada uno de los diferentes sectores tales como en la industria, economía, comercio, ocio y educación hasta el punto de resultar imprescindibles para la vida cotidiana.

Dado a los grandes avances producidos en las tecnologías de la información, así como las nuevas formas de comunicaciones electrónicas que surgen, tales como son: los mensajes enviados y recibidos mediante la utilización del correo electrónico y las aplicaciones de mensajería instantánea que tienen lugar a través de distintos soportes electrónicos, entre otras. Debido a ello, surge la necesidad de una reforma que se ha producido recientemente en la Ley de Enjuiciamiento Criminal con la finalidad de adaptarse a las necesidades de la sociedad tecnológica, mediante la Ley Orgánica 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, gracias a la que se produce la introducción de diligencias de investigación basadas en estos medios de comunicaciones telemáticas, en la interceptación y escuchas. Así aparece por primera vez la posibilidad de que estas diligencias se practiquen en los correos electrónicos y las aplicaciones de mensajería instantánea, tal y como es, *WhatsApp*, por parte de la Policía Judicial y la autoridad competente para la persecución de delitos que han tenido lugar a través de Internet conocidos como "ciberdelitos" para que mediante las mismas puedan servirse como fuente de prueba en el seno del procedimiento judicial en cuestión. A la vez, que regula la necesidad de una autorización pertinente por parte de la autoridad judicial competente para no vulnerar los derechos fundamentales consagrados en el artículo 18 de la Constitución Española que pueden producirse con la obtención de esta fuente de prueba para que pueda procederse de oficio.

Así pues, cada vez es más habitual la existencia de medios de prueba consistentes en *emails*, mensajería instantánea u otros medios basados en las nuevas

tecnologías quedando cada vez más obsoletos los tradicionales medios de prueba en los procesos judiciales.

Por ello, el presente trabajo tiene por el objeto el tratamiento completo y detallado de las pruebas de las nuevas tecnologías o prueba electrónica en el proceso penal y su incorporación al mismo, las garantías que han de darse para su admisión y su propio valor probatorio y, cuál sería el medio probatorio más adecuado según el caso.

De acuerdo con la reciente modificación en la Ley de Enjuiciamiento Criminal que no dispone ninguno de las caracteres citados en el párrafo anterior es importante esclarecer tales cuestiones así como la delgada de vulneración de los derechos fundamentales mediante la obtención y aportación de fuente de prueba por parte de las partes del artículo 18 de la Constitución Española como son el derecho a la intimidad o el derecho al secreto de las comunicaciones y la distinta protección legal y reiterada doctrina constitucional que los consagra.

La prueba de las nuevas tecnologías posee ciertas características notorias plenamente diferenciadas con el resto de tipos de prueba recogidas en nuestra Ley de Enjuiciamiento Civil. Con razón a la misma, han de darse todas las cautelas y profundizar de forma exhaustiva en las mismas, dado a la gran facilidad de manipulación que se produce en las comunicaciones telemáticas, examinando cuáles son los medios más apropiados mediante los que se garantice la autenticidad e integridad del medio probatorio del que se pretende servir.

En consonancia con lo anterior, es relevante resaltar la presencia en el proceso penal de estas nuevas tecnologías como medio de prueba a través de una mera fotocopia junto con el soporte electrónico en cuestión acompañado de la práctica de la prueba pericial informática, o bien, que sea propuesta su práctica por la contraparte con la finalidad de que se demuestre la autenticidad del contenido de la información. La dificultad de esta práctica varía en función del tipo de soporte electrónico que sea objeto de análisis siendo unos de mayor complejidad que otros.

Es por todo ello que se tiene como finalidad con el presente trabajo de realizar un análisis exhaustivo de los interrogantes más relevantes y de la transcendencia de la

escasa jurisprudencia en lo relativo a ésta. Así como clarificar las grandes lagunas que pueden surgir y surgen con respeto a la prueba de las nuevas tecnologías en el procedimiento penal, ya sea en lo relativo a la protección de los derechos fundamentales, la licitud de la prueba, la aportación de la misma con todas las cautelas, los medios que garantizan su integridad, los rasgos caracterizadores del contenido de este tipo de comunicaciones telemáticas y la práctica jurisprudencial de la misma.

Asimismo profundizando a rasgos generales en las particularidades que presentan los dos tipos de prueba tecnológica más frecuentes en el proceso penal, cómo es la incorporación al proceso y su admisión como medio de prueba de los correos electrónicos y de las conversaciones mantenidas a través del sistema de mensajería instantánea *WhatsApp*, así como la intervención por parte de oficio de los mismos, la prueba pericial y otros medios que garantizan la fehaciencia de la misma.

2. LA PRUEBA DE LAS NUEVAS TECNOLOGÍAS.

2.1. CONSIDERACIONES GENERALES.

2.1.1. El origen de la prueba de las nuevas tecnologías.

En las últimas tres décadas se ha vivido una rápida innovación en las tecnologías de la información más conocidas como TIC. La aparición de los teléfonos inteligentes y el transcurso de información a través de Internet a grandes velocidades han ido haciendo mella en todas las partes del mundo. Todas estas tecnologías están transformando a la sociedad viviendo actualmente lo que se denomina "sociedad de la información del conocimiento". Por lo tanto, hay que tener en cuenta que las comunicaciones telemáticas[1] han irrumpido en nuestras vidas de tal forma hasta el punto de considerarse indispensables en todos los ámbitos, incluido especialmente, el jurídico. Cada vez más

[1] Se denomina comunicación telemática al conjunto de servicios y herramientas que facilitan la relación interpersonal a través de Internet. Entre ellos se encuentra el correo electrónico o e-mail, que permite a sus usuarios enviar y recibir mensajes; el IRC *(Internet Relay Chat*), protocolo que facilita la comunicación textual e inmediata entre dos o más personas; y la mensajería instantánea, un programa con el que se pueden entablar conversaciones por voz, emplear vídeos y compartir diferentes tipos de archivos.
http://www.ite.educacion.es/formacion/materiales/142/cd/m3/recursos_tic_herramientas_de_comunicacin_telemtica.html(consultada 5 de marzo de 2016)

las personas usamos este tipo de comunicaciones desprendiéndonos de las que hace unos años atrás eran de lo más común tales como el envío de cartas, postales, etc. Sustituyéndose cada vez, con más frecuencia, por comunicaciones efectuadas a través de soportes electrónicos ya sea mediante aplicaciones de mensajería instantánea instaladas en el *Smartphone* como *WhatsApp* o mediante el envío o recepción de correos electrónicos efectuados desde el ordenador, entre otros. Como bien es cierto, éstas han supuesto grandes ventajas para realizar cualquier clase de actividades entre personas y fomentar el uso diario de la comunicación entre individuos que se encuentran a inmensas distancias a causa de su gran rapidez y fluidez inmediata pero, no en todos los sectores, pudiendo las mismas colisionar fácilmente con los derechos fundamentales recogidos en nuestra Carta Magna, y en particular los del artículo 18, tales como el derecho a la intimidad, honor y el secreto de las comunicaciones.

Por ello, hay que tener en cuenta que la irrupción de las nuevas tecnologías no puede dejar indiferente al Derecho ya que esta masiva expansión de las tecnologías y la conversión de forma habitual de nuestra concepción de la comunicación generan nuevos tipos de documentos que nuestra legislación debe contemplar para el correcto funcionamiento del procedimiento procesal penal.

Esta realidad que hoy nos ocupa, hace que cada vez con más asiduidad se aporten documentos que se encuentran recogidos en soportes electrónicos como medios de prueba al caso concreto[2].

Todo ello, nos lleva a la necesidad de hacer referencia a la prueba tecnológica [3] que encontramos regulada tanto la Ley de Enjuiciamiento Civil (LEC) como en la Ley

[2]Reconocido como tal en la Ley de Enjuiciamiento Civil en el Capítulo VI. De los medios de prueba y las presunciones, en el artículo 299.2 que regula los medios de prueba tecnológicos.

[3] Entendiendo por "prueba electrónica" o "tecnológica", la que permite acreditar hechos relevantes para el proceso, a través de los medios de reproducción de palabra, el sonido y la imagen, creados por los modernos instrumentos tecnológicos de la información. Se presenta en un soporte o documento electrónico, en el que se encierra un contenido informativo, el cual consta de dos elementos: uno material, el *hardware*, y otro lógico, su contenido, proporcionado por un *software* que contiene un programa informático determinado.

de Enjuiciamiento Criminal (LECrim) actualmente reformadas ambas para adaptarse al imponente desarrollo y expansión de las nuevas tecnologías como medio de comunicación tanto para las relaciones interpersonales como por su papel esencial para el desarrollo de actividades de diverso carácter que influyen en el sector financiero, laboral, mercantil, entre otros.

2.1.2 Regulación de la prueba de las nuevas tecnologías antes de la reforma de la Ley de Enjuiciamiento Criminal.

Antes de la reforma producida en la Ley de Enjuiciamiento Criminal no encontrábamos ninguna disposición que diera cobertura legal a este tipo de prueba, es decir, la regulación de la misma era totalmente insuficiente ya que en los tiempos que corren era imprescindible que se produjera esta reforma tanto en la LEC y LECrim para adoptarnos a las necesidades que la sociedad imperante demanda.

Autores como FUENTES SORIANO, resaltan la gran labor jurisprudencial y doctrinal para permitir que la legislación procesal penal, a pesar de las características decimonónicas que posee, sirviera de aplicación a la realidad actual. Así la misma dispone: "es lo cierto que un consolidado cuerpo de doctrina constitucional ha sentado las bases y los criterios a tener en cuenta para poder limitar los Derechos Fundamentales en el seno del proceso penal; y concretamente, por lo que ahora interesa, ha sentado las exigencias y requisitos básicos a tener en cuenta para la válida interceptación de las comunicaciones que sean estas de carácter "tradicional" o "tecnológico".[4]

Como bien se ha dicho la LECrim anterior a la reforma producida por la Ley Orgánica 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, los únicos preceptos que nombraban y regulaban este tipo de prueba se encontraban en la LEC, en la Ley Orgánica del Poder Judicial

---

Con más amplitud puede verse en DE URBANO CASTRILLO, E., "La regulación legal de la prueba electrónica: una necesidad pendiente (1), La Ley Penal, nº82, Mayo 2011, Editorial La Ley., p. 2.

[4] FUENTES SORIANO, O. (Coord.) "Comunicaciones telemáticas: práctica y valoración de la prueba"*El proceso penal actual*, Tirant lo Blanch, *en prensa*., p.3.

(LOPJ) y en la propia LECrim solamente hacía mención a dispositivos electrónicos sin entrar dentro de la cuestión.

Con respecto a la LEC cabe por destacar el artículo 299. 2 en cual se admite como medio de prueba y los preceptos más específicos del 382 al 384 en los que se establece que valor probatorio tienen los instrumentos de filmación, grabación y semejantes, el acta de reproducción y custodia de los materiales correspondientes y cualquier tipo de instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso.

La LOPJ en sus artículos 229.3 y 230.1 y 4 ambos sobre la utilización de dispositivos electrónicos tales como la videoconferencia o similares que sirvan de prueba para cualquier momento posterior.

Y, por último, en la LECrim los preceptos que hacen referencia a medios electrónicos es el art. 707 sobre las declaraciones de testigos de menores de edad o con discapacidad que podrán ser oídos mediante la utilización de tecnologías de la comunicación. También el art. 731 bis en el que se establece la posibilidad de empleo de videoconferencia para declarar y los artículos 743 y 788.6 sobre el acta electrónica del juicio oral. Si bien es cierto, en estos preceptos nada entran a regular específicamente las pautas, ni los caracteres generales de las pruebas de las nuevas tecnologías, sino que solamente se limita a hacer referencia a la posibilidad y a la actual utilización de dispositivos electrónicos durante el proceso penal que posteriormente puedan llegar a servir de prueba.

En definitiva, como se puede apreciar, existía una dispersión normativa y a la vez escasa de este tipo de prueba en estos tres textos normativos y sobre todo en la Ley de Enjuiciamiento Criminal en la que únicamente se hace referencia a los dispositivos electrónicos pero nada clarifica y aclara sobre estos medios, omitiendo cualquier posible utilización de las nuevas tecnologías en el ámbito de la investigación criminal, haciendo que cada vez más del uso de la jurisprudencia de los Tribunales juzgadores a la hora de entender estos medios presentes en el ámbito procesal penal.

2.1.3 La reforma efectuada por la LO 13/2015.

Nos encontramos ante una sociedad globalmente digitalizada en la que es habitual que, para desempeñar cualquier tipo de actividad, con independencia de su índole, el uso de las nuevas tecnologías. Tal cuestión no es baladí en el ámbito de lo jurídico debido a que el mismo constituye una parte de la realidad social y ha de adaptase a la misma para impartir justicia y garantizar el Estado de Derecho, haciendo así efectivos los postulados que en él se defienden y, a su vez, garantizando los derechos fundamentales e intereses que pueden colisionar con estos avances tecnológicos.

Antes de que se produjera la reforma, la Ley de Enjuiciamiento Criminal era un texto normativo absolutamente desfasado en el tiempo generando así una gran inseguridad jurídica y careciendo de respuesta a los problemas jurídicos que podrían surgir en lo relativo a las nuevas formas de delincuencia ligadas al uso de las nuevas tecnologías, como bien se establece en la exposición de motivos: "La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo (…)"[5].

Tras la reforma efectuada por la LO 13/2015 en nuestra ley procesal penal, estamos ante una normativa trascendente e innovadora que introduce el uso de medios tecnológicos para la investigación de delitos que hayan tenido lugar u ocasión a través de internet, es decir, introduce nuevas diligencias de investigación y establece la limitación de éstas para poder respetar de manera efectiva los derechos fundamentales que se puedan lesionar. Acabando así con las lagunas jurídicas y vacíos legales, actualizando términos que se encontraban desfasados tales como el término de investigado, introduciendo a su vez la figura del agente encubierto en internet; todas ellas con la finalidad de acabar con el anticuado sistema judicial, concediendo de la urgente y necesaria actualización para solventar todas estas deficiencias que se sufrían en el antiguo sistema procesal penal español, dotándolo de seguridad jurídica y haciendo efectivo el Estado de Derecho en el que vivimos.[6]

---

[5] Apartado IV del preámbulo de la Ley Orgánica 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.

[6] BUENO DE MATA, F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las

A continuación, se procede a analizar detenidamente cada uno de los aspectos que han sido determinantes de la reforma efectuada en la Ley de Enjuiciamiento Criminal:

En primer lugar, hay que tener en cuenta que esta Ley incide directamente sobre los derechos fundamentales recogidos en el art. 18 de la Constitución Española (CE) regulando las medidas limitativas de investigación tecnológica que puedan perjudicar a los derechos del ciudadano reconocidos en este artículo. A la vez, que refuerza los derechos procesales de los encausados y detenidos recogidos en el art. 24 CE.[7]

Por un lado, la cobertura legal que se da a las medidas de investigación tecnológica es objeto de atención en los Capítulos V a VII del Título VIII del Libro II de la LECrim y a todas ellas resultan de aplicación las disposiciones comunes introducidas en el Capítulo IV tales como: la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos de captación de la imagen, de seguimiento y de localización, el registro de dispositivos de almacenamiento masivo de información y el registro remotos sobre equipos informáticos. En otras palabras, nuevas diligencias de investigación tecnológica, al mismo tiempo que se actualiza a los nuevos tiempos, la detención y apertura de la correspondencia escrita en el art. 579 a 588 LECrim e introduce un nuevo artículo 579 bis relativo al tratamiento de los denominados "hallazgos casuales".

De acuerdo con el orden legal, establecido así en la Ley de Enjuiciamiento Criminal tras la reforma de la LO 13/2015, en relación con el art. 579 que consiste en la detención y posterior apertura de la correspondencia escrita y telegráfica con el fin de descubrir o comprobar hechos imputados a una persona, que tengan carácter delictivo. Puede adoptarse de la correspondencia remitida o recibida. Como bien establece este

---

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, p.1.

[7] Así lo establece en la propia Exposición de Motivos de la Ley en el apartado II: "esta Ley incide directamente en los artículos 18 y 24 de la Constitución Española, ya que introduce cambios jurídicos, sustantivos y procesales, que afectan al ámbito propio de la ley orgánica, en cuanto que desarrolla derechos fundamentales y libertades públicas recogidos en este precepto constitucional (…)"

artículo: "si hubiera indicios de obtener por estos medios del descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa (…)". Esta medida está limitada únicamente delitos de estimada gravedad recogidos en tal precepto y, siempre y cuando, se lleve a cabo a través de una resolución judicial previa que motive esta diligencia de investigación, salvo en aquellos casos que concurran razones de urgencia, que los ordenará el Ministro del Interior o el Secretario de Estado de Seguridad que ha de comunicárselo de forma inmediata al juez competente e incluso en ciertos casos en los que no se requiera autorización judicial como así se establece legalmente.

En lo relativo a los hallazgos casuales que recoge en el novedoso art. 579 bis, ha sido necesario su inclusión como consecuencia del resultado de la práctica de la detención y apertura de la correspondencia escrita y telegráfica en la que es frecuente que se halle información no incluida en el auto que habilita esa diligencia pero que pueda ser utilizado como medio de investigación o prueba en otro proceso penal que se encuentren relacionados entre sí.

En segundo lugar, con razón a la gran labor consagrada de la doctrina constitucional se encuentran regulados los principios rectores, que han de ser de aplicación a todas las diligencias de investigación tecnológica en el art. 588 bis a)como son los principios de especialidad [8], idoneidad, excepcionalidad, necesidad y proporcionalidad cuya concurrencia debe estar suficientemente acreditada, a la par que justificada en la resolución judicial, es decir, en el auto en que se decrete la medida, tanto como su extensión y naturaleza de la misma.

Estos principios son de obligado cumplimiento para garantizar la no conculcación de los derechos fundamentales, a su vez, ha se ser autorizada por el tribunal competente de acuerdo por el principio de jurisdiccionalidad la cual ha de sujetarse a una serie de contenido que dispone el art. 588 bis b) como son: el hecho qué es objeto de investigación, su concreción, las razones que justifiquen la necesidad e

8De acuerdo con Sala Primera. Sentencia 253/2006, de 11 de septiembre de 2006 (BOE núm. 243, de 11 de octubre de 2006).

idoneidad de la medida de acuerdo con el artículo anterior, los datos de identificación del investigado, la duración y la forma de ejecución de la misma, entre otros.

En relación con el principio de especialidad es realmente esencial ya que, conforme a él, se establece que se ha de tomar una medida que esté relacionada con un hecho concreto, determinado y definido.

De acuerdo con el principio de idoneidad, se ha de adoptar la medida más adecuada de manera objetiva y subjetiva al hecho delictivo que sea objeto de investigación, así como la duración.

Con respecto al principio de proporcionalidad la medida que se adopte debe corresponderse con el hecho cometido, su gravedad, y la condición del sujeto investigado.

La excepcionalidad y necesidad solo podrán acordarse cuando no se puedan implantar medidas menos gravosas para los derechos fundamentales del investigado y sean igualmente efectivas, a su vez, cuando no se tome esta medida nos encontremos ante dificultades para la correcta averiguación de los hechos que se quieran investigar.

En cuanto a lo relativo a la duración de las medidas de investigación, con carácter general, será de tres meses prorrogables hasta dieciocho meses (art. 586 bis e).

En tercer lugar, la interceptación de las comunicaciones telefónicas y telemáticas, son objeto de intervención los terminales o medios de comunicación que se traten de uso habitual o utilizados ocasionalmente por el sujeto investigado. También se podrá realizar su acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados recogidos en el art. 588 ter b.2[9] al proceso de comunicación en

[9]Entendiendo por datos de tráfico o asociados: "todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación de naturaleza análoga." https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725 (consultada el 17 de marzo de 2016).

los que el sujeto investigado participe tanto como emisor o receptor. En concurrencia, podrá interceptarse los terminales de los que sea titular el investigado cuando se dé un grave riesgo para su vida o integridad física, así como la comunicación de la que sea titularidad de una tercera persona cuando el sujeto investigado que utilice esa comunicación para cometer los hechos delictivos que sean objeto de investigación o, que se trate de una persona que colabore con el sujeto investigado, con la finalidad de ayudarle a conseguir los fines ilícitos que persigue.

Como es común en todas estas diligencias de investigación se requiere autorización judicial en el que se seguirá lo dispuesto en el artículo 588 bis b.

En esta medida cabe por destacar, el deber de colaboración de toda persona que contribuya a facilitar las comunicaciones a través del teléfono o cualquier otro medio o sistema de comunicación telemática están obligados a prestarla al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados todo lo necesario que se prescriba para la mejor eficacia de la medida, conforme al artículo 588 ter e.

Con respecto al control de la medida, la duración y solicitud de prórroga, se efectuará de acuerdo a las disposiciones comunes del art. 588 bis g, 588 bis e, 588 bis f respectivamente. Por tanto, respecto al control de la medida se encargará el Juez de instrucción cuya duración será de tres meses prorrogables hasta un total de dieciocho y la solicitud de prórroga se dirigirá por el Ministerio Fiscal o por la Policía Judicial al Juez competente que deberá cumplir con las exigencias de motivación de tal medida que se basen en los indicios del hecho que objeto de investigación.

Por lo que corresponde a los datos de tráfico o asociados de acuerdo con la legislación procesal penal se establece la posibilidad de acceder a los datos electrónicos conservados por los prestadores de servicios, la identificación del dispositivo mediante el *IP*, es decir, la captación de códigos de identificación del aparato o de sus componentes, que tiene la finalidad de que se pueda identificar a los usuarios, terminales y dispositivos de conectividad.

En cuarto lugar, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, recogidos en los artículos 588 quater a) a 588 quater e. Esta diligencia puede practicarse con autorización judicial motivada que habilite la captación y grabación de comunicaciones orales sobre todas aquellas comunicaciones en las que intervenga el investigado que se produzca tanto en la vía pública o en cualquier otro espacio abierto, así como en su propio domicilio o lugar cerrado.

La utilización de los dispositivos de captación y grabación de comunicaciones orales solo podrá solicitarse esta medida cuando los hechos que son objeto de investigación sean constitutivos de delitos graves tales los de terrorismo, los practicados en el seno de un grupo u organización criminal. Y que los dispositivos que se utilicen sean adecuados para el esclarecimiento de los hechos e identificar el autor.

En quinto lugar, la utilización de dispositivos de captación de la imagen, de seguimiento y de localización comprendido en los artículos 588 quinquies a) a c). Se caracteriza por la gran potestad que tiene la Policía Judicial ya que, sin necesidad de autorización judicial, podrán obtener y grabar por cualquier medio técnico imágenes del investigado en cualquier lugar público para interceptar los elementos del delito, los elementos relevantes para los hechos.

Sin embargo, para la utilización de dispositivos de seguimiento y de localización sí será preceptiva la autorización u orden judicial motivada por el Juez de instrucción competente y en la misma se detallará cuál será el medio tecnológico a utilizar, con la excepcionalidad, de que si se dan razones de urgencia, se establece la posibilidad de practicar la diligencia de investigación de forma inmediata para la clarificación o descubrimiento de los hechos investigados por parte de la Policía Judicial sin orden judicial que en el plazo de veinticuatro horas, como máximo, deberá comunicarlo a la autoridad judicial para que él mismo la ratifique o la cese.

De acuerdo con el artículo 588 quinquies c) en el que se establece la duración de la medida que será de tres meses como máximo desde la fecha de la autorización que será prorrogable hasta dieciocho meses cuando se acrediten los motivos que la justifican, es decir, el mismo plazo que el general.

En sexto lugar, el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) a c) cuando quepa la posibilidad de que en la ejecución de un registro domiciliario se pueda encontrar algún ordenador o cualesquiera otros dispositivos electrónicos que sean útiles para la investigación se han de incluir dentro de la resolución judicial que autorice el registro domiciliario que les habilite a acceder a ellos. También se prevé la posibilidad de acceder a estos dispositivos mediante la orden judicial motivada que tengan lugar fuera de un registro domiciliario. En casos de urgencia, se podrá prescindir de esta orden dándole traslado al Juez de instrucción competente dentro del plazo de veinticuatro horas desde que se ejecutó la medida para que sea ratificada o cesada en el plazo de setenta y dos horas.

La resolución judicial está sometida en estos casos a una serie de particularidades como son: el deber de no incautar los soportes físicos que no sean imprescindibles haciendo copia de los documentos que en él se hallen, la posibilidad de ampliación del registro a otros sistemas informáticos o parte del mismo, cuando existan las suficientes razones para pensar que los datos que se buscan se encuentran almacenados en otro sistema informático o parte de él, siempre que los datos que vayan a incautar se consigan de forma lícita o que la orden que habilitó el inicial; las autoridades y agentes encargados de la investigación se han de asegurar que se consagran con total integridad los datos hallados.

Y, en último lugar, el registro remoto sobre equipos informáticos (arts. 588 septies a) a c)) prevé la posibilidad de que el Juez competente pueda autorizar la utilización de datos de identificación y códigos, así como la instalación de un software que permita el examen a distancia y sin conocimiento del titular, de datos informáticos o base de datos pero sujetándose la adopción de la medida a los delitos que la ley hace referencia de forma expresa como son los cometidos en el seno de organizaciones criminales, de terrorismo, contra menores o personas con capacidad modificada judicialmente, contra la Constitución, de traición y relativos a la defensa nacional; y los delitos cometidos a través de instrumentos informáticos o similares de tecnología de la información.

La resolución judicial que se ha de adoptar, habrá de especificar los aparatos electrónicos u otros contenidos digitales, el alcance de la misma, cuáles y quiénes serán los agentes autorizados para su ejecución, la autorización, si fuera necesaria, para realizar y conservar copias de los datos informáticos.

En esta medida también se exige el deber de colaboración en su artículo 588 septies b. Y tendrá la medida una duración máxima de un mes prorrogable por iguales períodos de tres meses.

También en lo relativo al uso de las nuevas tecnologías, aparece la figura del agente encubierto en Internet, ha sido regulado por la necesidad de la persecución de determinadas modalidades delictivas derivadas del uso de las nuevas tecnologías gracias a esta ley, se prevé la posibilidad de que los agentes encubierto puedan obtener y captar imágenes y grabar conversaciones siempre y cuando reciba una autorización especial para que se puedan intercambiar archivos ilícitos que sean determinantes para la investigación que se lleve a cabo.

Y, finalmente, con respecto a la regulación de la prueba electrónica no se encuentra en la reforma efectuada recientemente, ningún precepto que regule cómo han de aportarse estas pruebas al procedimiento judicial, ni las cautelas que ha de llevarse a la hora de utilizar este tipo de comunicaciones electrónicas en juicio, remitiendo de este modo a los preceptos generales que recogen las formas de aportación y admisión de la prueba al proceso judicial.

2.2 LA INCIDENCIA DE LA PRUEBA DE LAS NUEVAS TECNOLOGÍAS AL DERECHO A LA INTIMIDAD, HONOR Y PROPIA IMAGEN, AL SECRETO DE LAS COMUNICACIONES EN EL ART. 18 DE LA CONSTITUCIÓN.

En la sociedad tecnológica actual nos vemos obligados a utilizar cualquier tipo de dispositivo electrónico ya que debido al impacto tecnológico de nuestro siglo ha cambiado progresivamente la forma de pensar, hacer e incluso de vivir. Se han convertido en medios prácticamente indispensables para las relaciones interpersonales en casi todos los ámbitos de la vida. Como bien se ha dicho anteriormente, estos medios

tienen grandes ventajas, pero a la vez, tienen un gran inconveniente en el ámbito jurídico de la persona, como es la delgada línea que se traspasa con gran facilidad a la hora de utilizar los dispositivos tecnológicos vulnerando los derechos fundamentales consagrados en el artículo 18 CE como son el derecho a la intimidad, al secreto de las comunicaciones y así se establece en el artículo 8.1 del Convenio Europeo de los Derechos Humanos del Consejo de Europa de 1950 (CEDH): "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia."

Con respecto a la concepción de los derechos fundamentales del art. 18.1, 2 y 3 CE[10]:

- Se entiende por derecho a la intimidad, aquel que se relaciona con lo más íntimo de la persona, en todos sus ámbitos de la vida, ya sea el familiar o el personal propio. Se encuentra ligado con la esfera más reservada de la vida personal e incluso se reconoce aquellas personas que tienen la consideración de "personajes públicos".

- Por derecho al honor, se entiende como el derecho que está relacionado con las circunstancias del tiempo y lugar en que se encuentra la persona. Éste habrá de valorarse de acuerdo con el carácter público de la persona, es decir, si es un personaje público o no, de cómo haya afectado tal comunicación a la vida personal del perjudicado, y de circunstancias en las que se haya producido y la repercusión que haya tenido. [11]

- La protección del derecho de las comunicaciones tiene una entidad propia, diferenciada de su vinculación con el derecho a la intimidad, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido, esto es, ya se trate de comunicaciones de carácter íntimo o de otro género. En efecto, según ha destacado la doctrina y la jurisprudencia, el art. 18.3 CE tiene un contenido puramente formal, protegiendo tanto de las intromisiones de los poderes públicos como de los particulares.[12]

---

[10] http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 (consultada el 26 de marzo de 2016)
[11] Véase en la STC 46/2002, de 25 de febrero.
[12] Véase en la STC 11/1984, de 29 de noviembre.

De acuerdo con la jurisprudencia del Tribunal Constitucional, el art. 18.3 CE consagra la libertad de las comunicaciones y garantiza su secreto, sea cual fuera la forma de interceptación, mientras dure el proceso de comunicación, en el marco de las comunicaciones indirectas, es decir, que empleen medios técnicos, y frente a terceros ajenos a la comunicación. [13] Además, en lo relativo al secreto se protege tanto el contenido íntegro, los sujetos que forman parte de la comunicación y cualquier otro elemento que forme parte de la comunicación.[14]

Sin embargo, en la práctica, la afectación a los derechos fundamentales que suele darse en relación a las comunicaciones telemáticas, ya sea mediante la intervención de diligencias de investigación tecnológica o mediante la proposición de medios telemáticos como prueba judicial a instancia de parte, es la del derecho a la intimidad y al secreto de las comunicaciones, a diferencia del derecho al honor, que sólo en determinados casos puede resultar afectado y atendiendo a determinadas circunstancias, que no son muy usuales con respecto a la comunicación electrónica.

A) Las diligencias de investigación tecnológica efectuadas por la Policía Judicial o la autoridad judicial competente:

Con respecto a ello, la doctrina constitucional ha consagrado una serie de principios rectores a la hora de adoptar cualquier diligencia de investigación que en la práctica pueda lesionar los derechos fundamentales de la persona, se encuentran regulados en el artículo 588 bis a) LECrim, con el que se autoriza de forma expresa la posibilidad de restricción de estos derechos fundamentales[15] siempre que cumplan una finalidad legítima y que gracias a esta limitación se obtenga un interés socialmente relevante. [16] Los principios que el artículo acuña: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad en la medida ya explicados en el

[13] Véase en la STC 70/2002, de 3 de abril.
[14] Véase en la STC 123/2002, de 20 de mayo.
[15]Véase a título de ejemplo la STC 37/1989, de 15 de febrero de 1989 (BOE núm.52 de 02 marzo)
http://hj.tribunalconstitucional.es/es/Resolucion/Show/1243 (consultada el 22 de marzo de 2016)
[16] Véase en la STC 37/89.

apartado anterior. Se trata de presupuestos constitucionales de obligado cumplimiento que, en el caso de ser vulnerados, dará lugar a la ilicitud de la prueba conforme el art. 11.1 LOPJ.

Sin olvidar, que toda limitación de derechos ha de ser adoptada con respecto a unas mínimas garantías que aseguran la fiabilidad del medio, la salud e integridad de la persona investigada. Asimismo, reiterada jurisprudencia del Tribunal Supremo lo dispone: "la tentación de saltar por encima de ella en aras de persecución de hechos delictivos debe ser administrada de manera prudente valorando los intereses afectados y acudiendo a vías de investigación alternativas cuando no sea indispensable la injerencia en el derecho fundamental.[17]

Atendiendo, a las diferentes medidas de investigación tecnológica que se pueden establecer, cabe la posibilidad de que si no llevamos en práctica todas las diligencias pertinentes podríamos acabar vulnerando distintos derechos fundamentales tales como el derecho al secreto a las comunicaciones y el derecho a la intimidad recogidos en el artículo 18.3 y 18.1 de la Constitución.

Las diligencias de investigación tecnológica en las que es de aplicación el principio de jurisdiccionalidad tales como: las de detención y apertura de la correspondencia, a la interceptación de las comunicaciones telemáticas y telefónicas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, registro de dispositivos de almacenamiento masivo de información y registros remotos sobre equipos informáticos. Únicamente puede darse esa limitación cuando se tramite la resolución judicial correspondiente y debidamente motivada por el Juez de Instrucción competente así lo señala el del Tribunal Supremo al establecer que " la decisión que se adopte en relación con la limitación de los derechos fundamentes debe ser decidida, en todo caso, por la autoridad judicial que instruye la causa y siempre bajo la ponderación de los intereses en conflicto evitando la lesión de las libertades cuando no sea aconsejable o proporcionada para los fines de la

[17]Véase en la STS 664/1994 de 25 de marzo (RJ 1994/2592)

investigación" [18] . Existiendo, por otro lado, dos salvedades en relación con la autorización judicial, como son los casos en los que concurra urgencia y se encuentre entre los delitos tasados que las podrá emitir el Secretario de Estado de Seguridad, una vez comunicada de forma inmediata y se proceda a su ratificación en un plazo máximo de 72 horas por parte de Juez competente, y en los casos en los que no afecte a la privacidad de las comunicaciones, es decir, al derecho al secreto de las comunicaciones[19] no será preceptiva la orden judicial motivada. Fuera de estos casos, si se incumple con el deber de la emitir la autorización judicial se incurrirá en un delito de revelación de secretos tipificado en el artículo 197 en su apartado II de nuestro Código Penal (CP), a la vez, que la prueba devendrá ilícita.

Cabe por destacar, que en lo relativo al derecho secreto de las comunicaciones, solo será legítimo la vulneración de tal "si está legalmente prevista con suficiente precisión, si está autorizada por la autoridad judicial en el curso de un proceso mediante una decisión suficientemente motivada y si se ejecuta con observancia del principio de proporcionalidad, es decir, si su autorización se dirige a alcanzar un fin constitucionalmente legítimo, como acontece cuando se adopta para la prevención y represión de delitos calificables de infracciones punibles graves y es idónea e imprescindible para la investigación de los mismos."

De acuerdo con el principio de especialidad dicha medida no puede dirigirse a prevenir delitos sino que deben de haber hechos que sean constitutivos de un delito para acreditar la efectiva limitación del derecho fundamental como sostiene el Tribunal Supremo "tales indicios han de ser entendidos, pues, como datos objetivos, que por su naturaleza han de ser susceptibles de verificación posterior, que permitan concebir sospechas que puedan considerarse razonablemente fundadas acerca de la existencia misma del hecho que se pretende investigar, y de la relación que tiene con el mismo la persona que va a resultar directamente afectada por la medida (...)" han de ser objetivos "en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control. Y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o se va a

[18]Véase en la STS 664/1994 (RJ 1994/2592).
[19]Véase en la STC 14/2001, de 29 de enero.

cometer el delito sin que puedan consistir en valoraciones acerca de la persona"[20].De acuerdo con ello, si así se decretará la prueba que se otorgue será considerada como prueba prohibida deviniendo en ilícita por contravenir con un derecho fundamental, produciéndose así la nulidad de dicha prueba.

Todas estas medidas son necesitadas del control judicial por parte del Juez de Instrucción que es el encargado de controlar la limitación de este derecho, su desarrollo y los resultados que produzca. En caso contrario, se entenderá como ilícita y carecerá de validez.

La cuestión relativa a la afectación de terceras personas, dispone el autor ASENCIO MELLADO[21] "la medida que se adopte no devendrá ilícita la que afecte a la interceptación de comunicaciones de sujetos a los que se investiga a través de atribuirle la condición de tal. No se trataría en este caso de un tercero, sino de un investigado que como tal debe ser tratado".

Y, por tanto, en cuanto a la destrucción de los registros del art. 588 bis, "una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del Secretario Judicial. Y se destruirá la misma cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o, cuando el delito o la pena, haya prescrito." De este modo, vemos como se garantiza la salvaguarda del derecho a la intimidad personal y familiar. Si ello, se incumpliera y el personal facultado hiciera uso de ellas en otros procedimientos.

Y, finalmente, en lo relativo a la duración de la medida se ha de adaptar a la finalidad de la misma y en caso de prórrogas han de estar motivadas, sin llegar a ser nunca prospectiva.

[20]Véase en la STS 893/2008 de 16 de diciembre (RJ 2009, 3054)
[21]ASENCIO MELLADO, J.M., *Derecho Procesal Penal,* Valencia, Tirant lo Blanch, 2015, p. 194.

En lo relativo, al derecho al secreto de las comunicaciones, consagrado en nuestra Constitución en el artículo 18.3 CE, cabe entender como bien dice nuestra jurisprudencia del Tribunal Constitucional "ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE"[22]

Según el Tribunal Constitucional, de acuerdo con su jurisprudencia, se protege la libertad de comunicaciones: "rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. El bien constitucionalmente protegido es así -a través de la imposición a todos del 'secreto'- la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje -con conocimiento o no del mismo- o captación de otra forma del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)... Y puede decirse también que el concepto de secreto que aparece en el art. 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como la identidad subjetiva de los interlocutores o de los corresponsales"[23]. Entendiendo, de este modo, que el artículo 18.3 protege tanto aquellas comunicaciones que no se refieren sólo al ámbito personal, lo íntimo o lo privado.

En cuanto, al derecho a la intimidad, del artículo 18.1 CE, el Tribunal Constitucional establece los requisitos que se han de dar para llevar a cabo la limitación de este derecho fundamental: "la existencia de un fin constitucionalmente legítimo (considerando como tal "el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal"); que la medida limitativa del derecho esté prevista en la ley (principio de legalidad); que como

[22]Véase en la STC 70/2002.
[23]Véase en la STC 114/1984.

regla general se acuerda mediante una resolución judicial motivada (si bien reconociendo que debido a la falta de reserva constitucional a favor del Juez, la Ley puede autorizar a la Policía Judicial para la práctica de inspecciones, reconocimientos e incluso de intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad) y, finalmente, la estricta observancia del principio de proporcionalidad, concretado en tres requisitos o condiciones: idoneidad de la medida, necesidad de la misma y proporcionalidad en sentido estricto."[24]

B) La aportación de la prueba tecnológica a instancia de parte:

Se entiende, que dicha prueba, no vulnera el derecho a la intimidad del art.18.1 CE, en el caso, de que sea una de las partes la que lo aporte al proceso que constituya en la comunicación electrónica como emisor o receptor de la misma, entendiendo así que tampoco se vulnerará el derecho al secreto de las comunicaciones del art.18.3 CE.

Ahora bien, si se entendería vulnerado el derecho a la intimidad, en el caso de que la comunicación que se divulgue contuviera rasgos de intimidad de una de las partes en la que se sienta coaccionado o presionado por la otra parte, asimismo lo establece lo establece reiterada jurisprudencia del TC incurriendo así en un delito regulado en el art. 197 CP, salvo que medio consentimiento por parte de alguna de las partes. Así lo dispone la doctrina, al decir que "la grabación de una conversación que tiene lugar entre dos personas y que uno de los intervinientes desea conservar para tener constancia fidedigna de lo tratado entre ambos, no supone una invasión de la intimidad (...) , es decir, "cuando una persona emite voluntariamente sus opiniones o secretos a un contertulio, sabe de antemano que se despoja de sus intimidades y se las trasmite, más o menos confiadamente, a los que le escuchan, los cuales podrán usar su contenido sin incurrir en ningún reproche jurídico."[25]

Por otro lado, en el caso de que un tercero ajeno a los interlocutores de la comunicación telemática "quien graba una conversación de otros, atenta, independientemente de toda otra consideración, al derecho reconocido en el art. 18.3

[24]Véase en la STC 207/1996, de 16 de diciembre.
[25] Véase en el Auto de la Audiencia Provincial de Madrid de 28 de abril de 2004 (LA LEY 99199/2004).

CE"[26]. Dicho de otro modo, atenta directamente contra el derecho al secreto de las comunicaciones.

Por tanto, la interferencia en la comunicación que se produzca por alguna de las partes que no sea el emisor o receptor de la misma, es decir, de cualquier otra persona, convertirá la prueba en ilícita y podrá ser este hecho constitutivo de delito del art. 197 CP.

2.2.1. La consideración de la prueba prohibida.

La prueba prohibida es aquella que resulta de la infracción de una norma de rango constitucional que consagra un derecho fundamental. Esta prueba puede darse en el seno de un proceso durante el desarrollo de la búsqueda y obtención de material probatorio que pretende ser incorporado por contener datos que son relevantes para el conocimiento y esclarecimiento de los hechos que son objeto de enjuiciamiento.[27]

Como bien establece en reiteradas ocasiones, el Tribunal Constitucional,ha afirmado la importancia y preferencia de los derechos fundamentales[28]. De ahí, que no surtirá efectos la prueba que contenga material o información que se haya obtenido vulnerando un derecho fundamental, devendrá ilícita y como consecuencia la imposibilidad de ser valorada y apreciada por el órgano jurisdiccional, así lo establece el artículo 11.1 LOPJ: "no surtirán efectos las pruebas obtenidas directa o indirectamente vulnerando los derechos fundamentales." Como también lo afirma la jurisprudencia del Tribunal Constitucional en numerosas sentencias, entre las que cabe por destacar, "nuestra jurisprudencia ha establecido también una prohibición absoluta de valoración de las pruebas obtenidas con vulneración de derechos fundamentales, de modo que los medios de prueba no pueden hacerse valer, ni pueden ser admitidos, si se han obtenido con violación de derechos fundamentales."[29]

[26] Véase en la STC 11/1984.
[27] ASENCIO MELLADO, J. M., *Derecho..." Op. Cit.*, pp.142-146.
[28] En la STC 114/1984 se reconoce la necesidad de alcanzar un justo equilibrio entre la actividad encaminada a la investigación y descubrimiento de actividades delictivas y la salvaguarda del conjunto de derechos que toda persona debe poseer en un Estado de Derecho.
[29] Véase en la STC 49/1996, de 26 de marzo.

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.