LA PRUEBA DIGITAL EN EL PROCESO PENAL.

CALIFICACIÓN: 10

JUSTIFICACIÓN: El trabajo presentado es el resultado de una excelente y minuciosa labor de investigación que demuestra que la autora es capaz de abordar las cuestiones más destacadas de la probática digital. El trabajo consigue exponer, de forma brillante y profunda a la vez, un análisis de la legislación, la jurisprudencia y la doctrina, integrando una amplia bibliografía. Asimismo, se identifican, plantean y desarrollan los problemas jurídicos más relevantes de esta novedosa materia así como la resolución de los mismos.

El trabajo posee una estructura ordenada en el que los diferentes epígrafes se relacionan unos con otros sin solución de continuidad. Además, la autora hace uso de un lenguaje claro y técnico propio de un jurista, siendo capaz de sintetizar la materia en un número de páginas limitado, pero sin que ello suponga descuidar el análisis de una variada y acertada selección de fuentes doctrinales de información.

Además, la inclusión de un caso práctico en el trabajo evidencia la capacidad de la alumna para confrontar sus conocimientos teóricos con la praxis real de la profesión, desarrollando y fundamentando con profundidad y detalle los diferentes problemas que plantea.

El resultado final que se nos presenta, por tanto, revela que la autora posee la capacidad de investigación que se le supone a un abogado, que domina la materia sobre la que versa el trabajo y que la misma es capaz de comunicar por escrito ese conocimiento, aptitud de extrema importancia para la práctica profesional de la abogacía.

Por todo ello, considero pertinente darle la máxima puntuación posible.

Marta Rodríguez Acosta

Tutor: Manuel Freddy Santos Padrón

Firmado digitalmente por: NOMBRE SANTOS PADRON MANUEL FREDDY - NIF 43770863T
Fecha y hora: 19.01.2018 14:50:44

TRABAJO DE FIN DE MÁSTER

MÁSTER UNIVERSITARIO EN ABOGACÍA

Curso 2017/2018

LA PRUEBA DIGITAL EN EL PROCESO PENAL

THE DIGITAL EVIDENCE IN CRIMINAL PROCESS

Marta Rodríguez Acosta

45897957 P

Tutor: Manuel Freddy Santos Padrón

RESUMEN. Los delitos cometidos a través de las nuevas tecnologías han aumentado de manera proporcional a los avances producidos en la materia, ello ha dado lugar a la transformación del proceso de investigación criminal, reflejado en cierta medida en la última reforma de la Ley procesal penal. En el presente trabajo estudiaremos la prueba digital en el proceso penal y la necesidad, en muchas ocasiones, de recurrir a la pericial informática para acreditar la autenticidad de la misma. Haremos especial hincapié en las fases de la prueba digital: la obtención de la misma y las vulneraciones de Derechos Fundamentales que pueden producirse en la obtención y que darán lugar a una prueba digital ilícita; la incorporación de la fuente de prueba al proceso; así como su valoración en el seno del mismo. También se examinará el cumplimiento de la cadena de custodia y las consecuencias de la manipulación y posterior aportación de esta tipología de pruebas al proceso.

ABSTRACT. Crimes committed through new technologies have increased which has changed the procedure of criminal investigation which has reflected to some extent in the latest reform of the Criminal Procedure Law. In this study we will look at digital evidence in the criminal investigation and the need to use IT experts to prove the authenticity of it. We will emphasise specifically on the phases of digital evidence. How obtaining it and the infringements of Fundamental Rights that may occur whilst obtaining the evidence and that could lead to an illicit digital evidence. This also includes the incorporation of the evidence source into the process, as well as its evaluation within it. Compliance with the chain of custody and the consequences of manipulation and subsequent contribution of this type of evidence to the process will also be examined.

ÍNDICE.

1. INTRODUCCIÓN.

"Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas", tal y como reza el considerando sexto de la Directiva 2002/58/CE [1]. Actualmente, como consecuencia del fenómeno de internet son muchas las personas que "viven en el entorno virtual" pues a través del mismo se difunde cultura, se puede disfrutar de un ocio sin ningún tipo de limitación, se entablan relaciones entre personas ya que surgen numerosas aplicaciones de ocio y comunicación online, las compras se hacen de manera rápida y sencilla a través del comercio electrónico, etc.,[2] en definitiva, son numerosos los aspectos de nuestras vidas que se desarrollan diariamente en dicho ámbito.

Como consecuencia de esta realidad, cada vez más predominante, se hace necesario articular una tutela judicial eficaz del entorno virtual, pues los avances derivados de las nuevas tecnologías (como el análisis de ADN, videocámaras, los programas informáticos rastreadores, los teléfonos móviles, la acústica forense, etc.) han ido aumentando en proporción al incremento de infracciones penales que se cometen mediante las nuevas tecnologías. Sirvan como ejemplo, el hacker que difunde un troyano en la red, el que profiere amenazas a otra persona a través de una red social, el que difunde en determinados foros pornografía infantil, o el que comete estafa a través de portales de internet, son algunas de las conductas que han tenido lugar como consecuencia de las nuevas tecnologías. Sin duda, puede afirmarse que internet se ha convertido en un nuevo instrumento para la comisión de hechos delictivos.

Así, en 2016, se conocieron 66.586 delitos cometidos en nuestro país a través de la red de los cuales el 68,9% lo constituyó el fraude informático y el 17,2% las amenazas y coacciones, consagrándose como los hechos delictivos más cometidos a través de este medio. Sin embargo, no fueron las únicas conductas que se perpetraron, también se cometieron delitos contra el honor, falsificación informática, acceso e interceptación

---

1 Ordoñez Solís, D. (2014) *La protección judicial de los derechos en internet en la jurisprudencia europea*. Madrid: Reus.

2 Gil Antón, A. (2015). "El menor y la tutela de su entorno virtual a la luz de la reforma del Código Penal LO 1/2015" en Revista de Derecho UNED nº16/2015. Rescatado de: http://e-spacio.uned.es/fez/eserv/bibliuned:RDUNED-2015-16-7070/menor_y_tutela.pdf

ilícita, delitos sexuales, interferencia de datos y delitos contra la propiedad industrial e intelectual.[3]

Estas realidades, por un lado el aumento en el uso de las nuevas tecnologías y, por otro, el incremento de conductas delictivas llevadas a cabo a través de las mismas, ha dado lugar a una transformación del proceso de investigación criminal. En concreto, la última reforma procesal de la Ley Orgánica 13/2015 de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, contempla la prueba informática y regula una serie de medidas de investigación en la fase de instrucción, como la utilización de dispositivos técnicos de captación de la imagen, seguimiento y localización, el uso del agente encubierto informático,… así como también se recoge, de manera exhaustiva, la incautación de equipos informáticos o dispositivos de almacenamiento de datos.

En definitiva, la finalidad de la mencionada reforma es dar cobertura legal a las citadas diligencias de investigación de delitos cometidos a través de la red y del uso de las nuevas tecnologías y, avalar así, que las mismas sean realizadas de manera garantista.[4] Sin embargo, a pesar de la reforma de la Ley procesal, el entorno virtual aún no tiene un adecuado reflejo en nuestro ordenamiento jurídico.

2. CONCEPTO Y REGULACIÓN DE LA PRUEBA DIGITAL.

2.1. Fuente de prueba y medio de prueba.

La distinción entre fuente y medio de prueba, hecha por CARNELUTTI[5] trata de resolver el problema de con qué se prueba. Las fuentes de prueba son conceptos preexistentes al proceso (la parte, el testigo, el documento, la cosa que ha de ser examinada, el conocimiento técnico del perito) y los medios de prueba son conceptos

[3] Ministerio del Interior: "Estudio sobre la cibercriminalidad en España." Recuperado de: http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf

[4] Bueno De Mata. F. (2015) "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica" Nº 8627, Diario La Ley

[5] Carnelutti, F (1982) *La prueba civil*. Buenos Aires: Depalma.

que existen en y para el proceso (interrogatorio de las partes o de testigos, reconocimiento judicial, dictamen de peritos, etc.). Digamos que las fuentes de prueba son los instrumentos que las partes deben averiguar para acreditar sus afirmaciones de hecho y que son, por definición ilimitadas. Los medios de prueba son los instrumentos de que el Juez se sirve para verificar las afirmaciones fácticas de las partes y son los previstos, con carácter limitados por el legislador.[6]

Como señala ABEL LLUCH[7], **en el proceso civil**, esa aparente contradicción entre el carácter ilimitado de las fuentes de prueba y el carácter limitado de los medios de prueba se resuelve recogiendo una enumeración de medios de prueba clásicos (en el art. 299.1 de la Ley de Enjuiciamiento Civil, en adelante LEC) comprensiva del interrogatorio de las partes, documentos públicos, documentos privados, dictamen de peritos, reconocimiento judicial e interrogatorios de testigos, positivando unos medios de prueba "modernos" (art. 299.2 LEC) comprensivo de los medios de reproducción de la palabra y sonido y de la prueba por soportes informáticos y abriendo las puertas a los medios de prueba futuros e innomidados, mediante la fórmula genérica del apartado 3 de ese mismo art. 299, a cuyo tenor: "Cuando **por cualquier otro medio no comprensivo previsto en los apartados anteriores** de este artículo pudiera obtenerse certeza sobre hechos relevantes, el Tribunal a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".

En el **proceso penal** español, precisa ABEL LLUCH[8], la investigación vigente se encomienda a la policía, la dirección de la investigación al Ministerio Fiscal y el control de la instrucción al Juez. Partiendo de la base de que en la investigación penal, cada vez es más habitual la incautación de equipos informáticos o de dispositivos de almacenamientos de datos, debemos determinar qué medios de prueba son los adecuados para introducirlos en el proceso penal.

Podemos afirmar entonces que, en el proceso penal y en la información contenida en equipos y dispositivos de almacenamiento, lo realmente relevante es el contenido y no el continente. Así por ejemplo, la información contenida en un equipo informático

---

6 Abel Lluch, X y Richard González, M (2013) *Estudios sobre prueba penal*. Madrid: Wolters Kluwer.
7 Abel Lluch, X (2013) *Estudios sobre prueba penal*… Op. Cit.
8 Abel Lluch, X (2013) *Estudios sobre prueba penal*… Op. Cit.

puede acceder al proceso a través del reconocimiento del investigado, a través de la declaración de los testigos, a través de su impresión en papel, o a través de un informe pericial informático.

Aunque abundaremos sobre ello más adelante, conviene aclarar que la acreditación de la autenticidad e integridad de la fuente de prueba es la llamada "doctrina de la cadena de custodia". Lo que implica que en la instrucción deben adoptarse todas las medidas para que las fuentes de prueba –en este trabajo, las derivadas de la prueba digital o nuevas tecnologías- acceden al proceso en el mismo estado en que fueron obtenidas, sin alteraciones ni manipulaciones para que quede preservada su autenticidad y puedan ser valoradas por el órgano competente de enjuiciamiento.

También conviene distinguir desde ahora, respecto al análisis pericial de los contenidos de los archivos informáticos, entre la pericial referida a la fuente de prueba y la pericial referida al contenido de la prueba. La primera, sobre la fuente de prueba, tiene por finalidad dictaminar que se trata de la misma de fuente de prueba (garantía de la autenticidad) o que la misma no ha sido manipulada o alterada (garantía de la integridad, mediante el *hash*). La segunda, sobre el contenido de la fuente de prueba, puede tener mayor casuística, como por ejemplo, autenticidad del software, infracción de derechos de propiedad intelectual, sobre archivos encriptados, ocultos o eliminados.

2.2. Problemática general de la prueba digital.

Para definir la prueba electrónica, haremos alusión en primer lugar al concepto de documento electrónico que, conforme al artículo 3.5 de la Ley de Firma Electrónica 59/2003, de 19 de diciembre, es "la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado". [9]

[9] Carrasco Mayans, S. (2016) "La alegalidad o limbo legal de la prueba electrónica" en *La prueba electrónica: validez y eficacia procesal*. Recuperado de: http://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf

El documento electrónico, a su vez, y tal y como dispone el citado precepto, será soporte de documentos públicos (firmados electrónicamente por funcionarios que tengan atribuida la facultad de dar fe pública), documentos privados y documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones, entre otros.

El documento electrónico se realiza en un lenguaje binario, que se traduce en lenguaje alfabético común. Por lo que, entre lo conservado y lo exteriorizado no existe identidad, pues el archivo se conserva en sistema binario mientras que el texto exteriorizado es fruto de la transformación de ese sistema binario en forma de escritura con letras del alfabeto.[10]

Así, cualquier tipo de información, que ostenta valor probatorio y está contenida en un medio electrónico o es transmitida por dicho medio, es lo que constituye la prueba digital. A su vez puede diferenciarse entre dos modalidades de prueba digital: la información que se contiene en dispositivos electrónicos y la información que se transmite a través de redes de comunicación.[11]

Como ya dijimos en el apartado referido a las fuentes de prueba y medios de prueba, también la LEC, en el artículo 299, contempla la posibilidad de que las partes, en el marco de un proceso, aporten pruebas digitales y las describe como "los medios de reproducción de la palabra, el sonido y la imagen, así como a los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso". [12]

A pesar de que contamos en la actualidad con diversidad de herramientas y técnicas que permiten garantizar la veracidad, origen y exactitud de la información contenida en un

---

[10] García Torres, M. (2011). "La tramitación electrónica de los procedimientos judiciales, según la Ley 18/2011, de 5 de junio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil." Recuperado de https://dialnet.unirioja.es/descarga/articulo/4405667.pdf

[11] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: Wolters Kluwer.

[12] Muñoz Sabaté, L (2017) *Técnica probatoria*. *Estudios sobre las dificultades de la prueba en el proceso*. Madrid: Wolster Kluwer.

documento electrónico, en numerosas ocasiones, para dotar de validez a las mismas en el marco de un proceso judicial se requiere de la intervención de personal cualificado como peritos informáticos y notarios.

Así, cuando hablamos de pruebas electrónicas, el Tribunal Supremo exige la constatación de la existencia del hecho a través de periciales informáticas cuando aquellas sean contradichas. Sin embargo, ello no implica que sólo sea válida la prueba digital que haya sido confirmada por perito informático. Por tanto, en lo concerniente a pruebas digitales aportadas por las partes, se estará a lo dispuesto en el artículo 326.1 de la Ley de Enjuiciamiento Civil que dispone que los "documentos privados harán prueba plena en el proceso en los términos del artículo 319, cuando su autenticidad no sea impugnada por parte de a quien perjudiquen."

Dispone el Alto Tribunal en STS 224/2017, de 8 de marzo, que la posibilidad de manipulación de la prueba fundada en una comunicación bidireccional mediante sistemas de mensajería instantánea "forma parte de la realidad de las cosas", pues tales sistemas permiten la creación de cuentas de manera libre y garantizan el anonimato del usuario. En consecuencia, es posible la creación de cuentas con una identidad simulada y "aparentar una comunicación en la que un único usuario pueda relacionarse consigo mismo". Por ello, en el proceso penal, este tipo de pruebas habrá de abordarse con extremada cautela.

Precisa la mencionada sentencia que la impugnación de este tipo de conversaciones requiere la adopción de ciertas prevenciones cuando son aportadas o introducidas en el proceso mediante archivos impresos y "desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria". En caso de que tal medio probatorio se impugnase, y se suscitasen dudas razonables sobre de su certeza y autenticidad, será necesario la práctica de una prueba pericial informática que identifique el origen de la comunicación, la identidad de los interlocutores y la autenticidad de su contenido.

En definitiva, la autenticación únicamente se requiere en casos de impugnación del documento, pues, mientras no sea impugnado, éste se tendrá por bueno.[13]

[13] Muñoz Sabaté, L (2017) *Técnica probatoria*… Op. Cit.

3. FASES DE LA PRUEBA DIGITAL.

3.1. Obtención de la prueba.

La prueba puede obtenerse por las partes, y ser éstas quienes la aporten al proceso o puede ser la policía quien, en el marco de una investigación, obtenga la misma para posteriormente aportarla al proceso. En este último caso, se precisará autorización judicial si con tal obtención pudieran resultar vulnerados derechos fundamentales del sujeto que está siendo investigado.

La nueva redacción dada a la Ley de Enjuiciamiento Criminal, en adelante LECrim, regula la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital y de acceso a repositorios telemáticos de datos, es decir, contempla todos los dispositivos o instrumentos que sirven de soporte para el almacenamiento masivo de datos.

Así mismo, la ley prevé que la información digital pueda encontrarse deslocalizada, por lo que los datos podrían no solo estar almacenados en los dispositivos físicos sino que podrían estar alojados en servidores, como la nube.[14]

Como se desarrollará a lo largo del epígrafe, la obtención de la prueba digital es una cuestión que genera no pocas dificultades dado que la misma puede encontrarse en un dispositivo electrónico, y este dispositivo podría hallarse en un lugar cerrado por lo que se requerirá entrada y registro en el mismo para la aprehensión del mismo y, a su vez, la información contenida en él puede haber sido encriptada o eliminada, por lo que se precisará, a su vez, de prueba pericial informática para conocer el contenido del mismo. También existe la posibilidad de acceder al contenido de un dispositivo electrónico mediante registros remotos, por lo que no siempre es necesaria la aprehensión física del dispositivo.

[14] López Barajas Perea, I. (2017). "Nuevas Tecnologías aplicadas a la investigación penal: el registro de equipos informáticos" en *Revista de Internet, Derecho y Política*.

3.1.1. Obtención de la información obrante en dispositivo electrónico a través de la aprehensión del mismo.

Para la obtención de la prueba digital, la LECrim contempla dos fases, la fase de incautación o aprehensión del dispositivo electrónico y la fase de acceso al contenido del mismo.

Así, por un lado, para incautar un dispositivo electrónico que se encuentre en un lugar cerrado se precisará de una entrada y registro en el lugar, para lo cual se requerirá autorización judicial y, para que tal autorización pueda ser concedida, "deben existir indicadores razonablemente acreditados que permitan relacionar al titular o titulares de la vivienda que trata de registrarse con las acciones criminales objeto de investigación", tal y como reza la STS 163/2015 de 24 de marzo.

En concreto, el auto que autorice la entrada y registro debe fundamentar necesariamente y, a tenor de lo dispuesto en el Auto AP Barcelona 95/2017 de 13 de febrero: "a) el grado de sospecha necesario para decretar la medida, es decir, que pudieran decretarse pruebas de la perpetración delictiva o de que estas pudieran resultar destruidas, b) la demostración de que existen elementos suficientes desde el punto de vista de la experiencia criminalística para fundar la sospecha de comisión del delito, c) la naturaleza y gravedad de los hechos investigados, d) la relación con la persona afectada por la medida, e) la indicación de si la misma es adoptada en el curso de un proceso judicial abierto o si tiene origen en una petición policial producida también en el seno de las diligencias policiales de investigación que habrían de determinar la apertura de un proceso judicial por sí mismo en averiguación del presunto delito, f) requiere una ponderación caso por caso de las circunstancias (…)." Pero también, como dispone la citada resolución, y la STS 404/2016 de 11 de mayo, se estima suficiente, como fundamentación fáctica, para decretar este tipo de autos, la remisión a los antecedentes obrantes en las actuaciones y en la solicitud policial.

Es habitual que, bajo el paraguas de la resolución que autoriza la entrada y registro, se proceda a la incautación de los dispositivos electrónicos hallados en el mismo. Así, dispone la STS 786/2015, de 4 de diciembre, "no pocas resoluciones hacen extensiva la

habilitación judicial concedida para la intromisión domiciliara a la aprehensión de todos aquellos soportes de información que pueda encontrarse en el interior de la vivienda."

Tal y como dispone la jurisprudencia, la entrada y registro en un domicilio sin la autorización judicial correspondiente solo es loable con el consentimiento de su titular o en caso de flagrante delito. Por lo que, de no darse estos dos supuestos mencionados, se precisará necesariamente de autorización judicial que justifique la necesidad de la medida.

Sin embargo, no todo lugar cerrado constituye domicilio, puesto que se excluyen de dicho concepto todos los lugares donde no se desarrollan actos de la vida privada, aunque el titular puede estar legitimado para no autorizar la entrada o permanencia de terceros, tal y como reza el Auto de la Audiencia Provincial de Barcelona antes citado.

Por otro lado, para el caso de que se requiera el acceso a la información obrante en un dispositivo electrónico que no se halla en lugar cerrado sino que, por el contrario, está en posesión de una persona o ha sido hallado o descubierto, ha de contarse bien con la autorización del propietario del dispositivo, bien con la correspondiente autorización judicial. La Policía Judicial también podrá actuar sobre el mismo sin necesidad de que se den los dos supuestos anteriores en los casos en que la urgencia lo requiera.[15]

En ambos casos, tanto si el dispositivo electrónico se encuentra en un domicilio o lugar cerrado, como si está en posesión de alguien o ha sido descubierto, será necesario, para el acceso a la información contenida en él, autorización judicial o consentimiento del titular del dispositivo, dado que el acceso a los datos contenidos en el mismo podría conculcar derechos fundamentales convergentes, tales como el derecho a la intimidad, al secreto de las comunicaciones, etc.

Cabe resaltar, como ya se aventuró, que la incautación de un dispositivo electrónico no ampara también el visionado del contenido del mismo, sino que se requiere autorización judicial expresa. Y así lo dispone el artículo 588 sexies a) de la LECrim cuando dispone que si con la práctica de un registro domiciliario se prevé la aprehensión de

[15] Delgado Martín, J. (2013) La prueba electrónica en el proceso penal. *Diario La Ley*, Sección Doctrina. La Ley.

dispositivos electrónicos tales como ordenadores, dispositivos de almacenamiento masivo de información, instrumentos de comunicación telefónica, etc., **"la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos**. **La simple incautación de cualquiera de los dispositivos** a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, **no legitima el acceso a su contenido**, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente."

Por otro lado, "el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno" (STC 83/2002, de 22 de abril) e impedirá considerar vulnerado dicho ámbito.

Bastará, por tanto, con el consentimiento para el acceso al contenido del dispositivo. Y dicho consentimiento no ha de ser necesariamente expreso, ya que la jurisprudencia otorga eficacia al consentimiento otorgado de forma tácita (STS 786/2015, de 4 de diciembre).

Sin embargo, hay jurisprudencia que entiende que cuando no medie consentimiento del titular del dispositivo electrónico, así como tampoco autorización judicial, podrá ser visionada la información contenida en el mismo siempre que ésta esté "motivada por la concurrencia de otros bienes jurídicos constitucionalmente protegidos de forma que se aprecie una **justificación objetiva y razonable para la injerencia en su derecho a la intimidad personal**." Así, la actuación de la policía en el marco de investigaciones dirigidas al esclarecimiento de un delito, que consista en el acceso a los datos obrantes en el continente sin la pertinente autorización judicial, estaría justificada por la existencia de otros bienes jurídicos constitucionalmente protegidos (STS 786/2015 de 4 de diciembre).

3.1.1. Obtención de la información obrante en el dispositivo electrónico mediante registro remoto del mismo.

Cabe la posibilidad de acceder a los datos o información contenida en un dispositivo electrónico mediante la instalación en el sistema del investigado de un software o, sin necesidad de instalar programa alguno, mediante la utilización de códigos. [16]

Así lo contempla la LECRim, en el artículo 588 a) septies, donde regula el acceso a los dispositivos sin necesidad de aprehender los mismos mediante la utilización de códigos o instalación de software que permitan el examen de forma remota y telemática del dispositivo electrónico, todo ello sin conocimiento del titular del mismo. Sin embargo, estos registros remotos solo se contemplan para investigar una serie de delitos: "a) delitos cometidos en el seno de organizaciones criminales, b) delitos de terrorismo, c) delitos cometidos contra menores o personas con capacidad modificada judicialmente, d)delitos contra la constitución, de traición y relativos a la defensa nacional y, e) delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o telecomunicación o servicio de comunicación."

Ahora bien, el registro remoto de un dispositivo electrónico, sólo se ejecutará en caso de necesidad y de manera excepcional. Así, podrá acordarse cuando no pueda investigarse el delito por medio de otras medidas menos gravosas y de menor afección a los derechos fundamentales del investigado que también permitan la investigación del hecho así como cuando la comprobación del hecho, la averiguación del autor o de su paradero así como otros hechos determinantes se vean impedidos u obstaculizados sin la utilización de esta medida, y así lo regula el artículo 588 bis a) de la LECrim.

La obtención de información relevante para el proceso penal mediante este tipo de técnicas es necesaria cuando se requiere una actuación rápida sin embargo, dado que se pueden ver conculcados ciertos derechos fundamentales tales como el derecho a la intimidad o el derecho a la protección de datos personales, para poder ejecutarse el registro remoto, se precisa en todo caso autorización judicial. Autorización que se

[16] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en*…Op. Cit.

otorgará a raíz de solicitud por parte del Ministerio Fiscal o de la Policía Judicial, aunque también podrá decretarla el juez de oficio.

La solicitud de tal medida requiere de un contenido mínimo sujeto a lo dispuesto en el art. 588 bis b) LECrim, así los aspectos necesarios de tal petición son: "la descripción del hecho objeto de investigación, la identidad del investigado si se conociere, la exposición de la necesidad que justifique la medida, conforme al art. 588 bis a) y los indicios de criminalidad que se hayan puesto de manifiesto, los datos de los medios de comunicación empleados que permitan la ejecución de la medida, la extensión de la medida con especificación de su contenido, la unidad investigadora de la Policía Judicial que se hará cargo de la intervención, la forma de ejecución de la medida, la duración de la misma y el sujeto que llevará a cabo la medida", si se conociere. Además, la solicitud se sustanciará en pieza separada y secreta.

Finalmente, dispone la LECrim, la resolución que acuerde la ejecución del registro remoto especificará los dispositivos electrónicos objeto del mismo, las medidas necesarias para conservar la integridad de la información contenida en los mismos, y tendrá una duración de un mes, prorrogable hasta tres.

Se trata de un método útil cuando el dispositivo electrónico se encuentra en movimiento continuamente, o para el caso de que el acceso al lugar cerrado donde se halla el mismo pudiera suponer un riesgo para la integridad física de los agentes, así como cuando es preciso acceder al equipo en vivo para descifrar las claves utilizadas, por ejemplo.[17]

En síntesis, la LECrim regula dos fases para la obtención de la prueba digital, la primera referida a la requisa del dispositivo electrónico y la segunda relativa al acceso al contenido obrante en el mismo. Para incautar el mismo se precisará de autorización judicial si el mismo se encuentra en domicilio o lugar cerrado. Así como también se requiere autorización judicial cuando se trata de acceder a los datos contenidos en el dispositivo, dado que podrían verse quebrantados derechos fundamentales con tal acceso. Esta regla no operará en caso de que el titular del mismo preste su consentimiento para que sea visionado o, en los casos extraordinarios de extremada

[17] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en*…Op. Cit

urgencia en los que la Policía Judicial podrá efectuar el visionado, comunicándolo posteriormente al Juez.

3.1.3. Obtención de la información mediante la figura del agente encubierto informático.

La LECrim, en el art. 282 bis, regula la posibilidad de que el Juez de Instrucción o el Ministerio Fiscal (informando al Juez de manera inmediata), autoricen, mediante resolución motivada, a funcionarios de la Policía Judicial para "actuar bajo identidad supuesta, adquirir y transportar los objetos del delito y diferir la incautación de los mismos". Lo que se contempla en el mencionado precepto es la figura del agente encubierto, a la que se podrá recurrir para la investigación de una serie tasada de delitos y enumerada en el art. 282 bis 4 LECrim: delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos; delitos de secuestro de personas; delitos de trata de seres humanos; delitos relativos a la prostitución; delitos contra el patrimonio y el orden socioeconómico; delitos relativos a la propiedad industrial e intelectual; delitos contra la salud pública y; delitos de terrorismo, entre otros.

Sin embargo, en ocasiones, para la investigación de determinados delitos cometidos a través de dispositivos electrónicos conectados a la red, será preciso recurrir a la figura del agente encubierto informático. El agente encubierto informático puede ser definido como el funcionario público que se infiltra en la Red con el objetivo de recabar información sobre determinados hechos ilícitos producidos en la misma y, su autoría.[18] Infiltración que, en este caso, únicamente podrá ser autorizada por el Juez de Instrucción.

El agente encubierto informático, además de poder investigar los delitos reseñados en el art. 282 bis LECrim, podrá investigar los delitos contemplados en el art. 579.1 LECrim: "delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal y; delitos de

[18] Bueno de Mata, F (2012). *El Agente cubierto en internet: mentiras virtuales para alcanzar la justicia*. Recuperado de: https://dialnet.unirioja.es/servlet/articulo;jsessionid=4A7CF70253AEF84F98D8F7F8C4BCD955.dialnet01?codigo=4036206

terrorismo". Por lo que se amplía el catálogo de delitos susceptibles de investigación cuando media actuación del agente encubierto informático.

El agente tratará de inmiscuirse en las comunicaciones mantenidas en canales cerrados de comunicación por medio del engaño, mediante la asignación y utilización de una identidad ficticia. Así, se integra en el seno de un grupo cerrado de usuarios cuya finalidad es compartir entre los miembros del mismo, información que pudiera ser relevante para esclarecer el hecho, archivos que podrían probar la comisión del hecho delictivo, la autoría del mismo, etc. La Ley permite, en estos supuestos, que el agente intercambie o envíe archivos ilícitos, ello es así debido a que, frecuentemente, es requisito para el ingreso en los citados grupos cerrados la aportación de este tipo de material ilícito. Toda vez que si el agente no comparte con el grupo de usuarios tales archivos, no conseguiría entrar en el mismo y, la investigación no resultaría fructífera.[19]

Este intercambio o envío de archivos se torna necesario especialmente en materia de pornografía infantil, ya que los consumidores de la misma interactúan en foros muy restringidos de usuarios y de difícil acceso. Motivo por el cual, la puesta en circulación de material de esta índole por parte del agente encubierto es de suma importancia para obtener la confianza del investigado. Confianza que, incluso, puede llegar a surgir de la calidad del material enviado. Sin embargo, ello no implica que el intercambio de archivos de esta naturaleza constituya la actuación ordinaria del agente, sino que, por el contrario, se requerirá autorización específica previa a tal actuación.[20]

Así, conforme a la previsión del art. 282 bis LECrim y, en relación con lo dispuesto en el art. 579.1 LECrim, el agente encubierto informático ha sido utilizado en España para la investigación de delitos de terrorismo. En la Sentencia de la Audiencia Nacional nº 3/2017, de 17 de febrero, se describe la actuación de infiltración del agente encubierto que rastrea las redes sociales en las que obraban perfiles con publicaciones a favor de grupos terroristas y diversos foros de armas. El agente detecta en *Facebook*

---

[19] Valverde Mejías, R. *Cuestiones procesales relativas a la investigación de los delitos en red*. Fiscalía General del Estado. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a.

[20] Fernández López, M. (coord.). (2017). *Justicia penal y nuevas formas de delincuencia*. Madrid: Tirant lo Blanch.

publicaciones con contenidos del Daesh y de odio a España y, entabla amistad con individuos miembros de los grupos en los que se publican tales contenidos, a partir de que se gana la confianza de los usuarios implicados, uno de ellos le propone llevar a cabo un atentado a la vez que le comunica su intención de atentar en España contra la policía. El testimonio del agente encubierto posibilitó la investigación de los hechos y final detención de los implicados.

3.1.4. Posible vulneración de derechos fundamentales en la fase de obtención de la prueba digital con repercusión en el proceso penal: la prueba digital ilícita.

A pesar de que en los apartados expuestos se ha hecho referencia a la obtención de la información obrante en dispositivos electrónicos a través del examen de los mismos y, la correspondiente pericial informática, en su caso, así como la obtención de información a través del agente encubierto, o del examen de los datos hallados en la nube, es evidente que no son las únicas formas de acceder a datos que pudieran tener especial relevancia para la investigación criminal. Así, existen otros medios de investigación criminal como pueden ser la interceptación de las comunicaciones, la grabación directa de comunicaciones orales así como la captación de la imagen o el uso de dispositivos de seguimiento y geolocalización igualmente aptos para llevar a cabo la investigación criminal. En el presente epígrafe examinaremos la posibilidad de que estas medidas de investigación criminal puedan atentar contra los derechos fundamentales del investigado.

En función de la diligencia de investigación utilizada para la averiguación del hecho delictivo, podrían verse afectados unos derechos fundamentales u otros.

Así, cuando la policía obtiene las fuentes de prueba a través de las escuchas telefónicas de conversaciones entre particulares sometidos a investigación penal, podría verse conculcado el derecho al secreto de las comunicaciones regulado en el artículo 18.3 CE. Dispone la Sentencia del Tribunal Constitucional núm. 170/2013, de 7 de octubre que, "el secreto de las comunicaciones se predica de lo comunicado, sea cual sea su contenido". El objeto de la protección de este precepto – aduce la referida sentencia –

"es el proceso de comunicación en libertad y no por sí solo el mensaje transmitido, cuyo contenido puede ser banal o de notorio interés público".

Por otro lado, con el acceso y visionado de la información obrante en un dispositivo móvil, un disco de almacenamiento portátil, o cualquier otro dispositivo electrónico, podría injerirse en el derecho a la intimidad personal regulado en el artículo 18.1 CE. La sentencia antes mencionada define la intimidad constitucionalmente protegida como "un concepto de carácter objetivo o material, mediante el cual el ordenamiento jurídico designa y otorga protección al área que cada uno se reserva para sí o para sus íntimos, un «ámbito reservado de la vida de las personas excluido del conocimiento de terceros» en contra de su voluntad."

El acceso a los datos contenidos en dispositivos electrónicos indudablemente afecta al derecho a la intimidad personal, pero podría también afectar al secreto de las comunicaciones cuando exista un proceso de comunicación, es decir, cuando dichos dispositivos sean usados para transmitir información entre un transmisor y un receptor a través de redes de comunicación como mensajería instantánea o a través de correo electrónico.[21]

Sin embargo, no se vulnerará el derecho al secreto de las comunicaciones en los procesos de comunicación ya celebrados y concluidos, ya que no se está, en estos casos, ante un proceso de comunicación en sí, sino que en tales supuestos el derecho conculcado podría ser el derecho a la intimidad personal por verse afectado el ámbito reservado de la vida personal de los investigados.[22] Y, en este sentido se pronuncia la STS 864/2015 de 10 de diciembre estimando que "el derecho al secreto de las comunicaciones rige mientras se desarrolla el proceso de comunicación, una vez cesado este, llegado el mensaje al receptor, salimos del ámbito del art. 18.3 CE , sin perjuicio, en su caso, del derecho a la intimidad proclamado en el número 1 del mismo precepto".

La incorporación al proceso de datos financieros, fiscales, de comunicaciones telemáticas, etc., obtenidos durante la investigación pudiera atentar contra el derecho regulado en el art. 18.4 CE, el derecho a la protección de datos personales o a la autodeterminación informativa. El objeto del mencionado derecho, como define la STC

[21] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en…*Op. Cit.
[22] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en…*Op. Cit.

199/2013 de 5 de diciembre "no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o intima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo."

Debe precisarse que, conforme a lo dispuesto en el art. 236 quáter de la Ley Orgánica del Poder Judicial, en adelante LOPJ, no es necesario el consentimiento previo del titular del derecho para el tratamiento de sus datos personales por los Tribunales en ejercicio de la potestad jurisdiccional.[23] Tampoco se requerirá el consentimiento del titular del derecho para ceder los datos a las Fuerzas y Cuerpos de Seguridad (supuesto regulado en el art. 22 LOPD) cuando la petición de datos esté en relación con una concreta investigación criminal. En estos casos, el responsable de la policía que efectúa tal petición debe quedar identificado en aras a poder analizar, si fuese necesario, si la misma se ajustaba a la ley.[24]

Por último, y en relación con la actuación del agente encubierto informático, para el caso de que tal actuación no estuviese amparada en la correspondiente autorización judicial, podrían verse conculcados una serie de derechos. Dado que, como ya

[23] Informe sobre la petición formulada por la Agencia Estatal de la Administración Tributaria para que se remita a dicha Agencia información con trascendencia tributaria obrante en los órganos jurisdiccionales. Del gabinete técnico del CGPJ. Recuperado de: http://daascompliance.es/wp-content/uploads/2017/09/Acuerdo-CGPJ-20-7-2017.pdf (El Consejo General de la Abogacía Española ha recurrido este acuerdo del CGPJ y pedido la suspensión cautelar del mismo).

[24] Informe nº10/2014 del gabinete jurídico de la Agencia Española de Protección de Datos. Recuperado de: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2014-0010_Cesi-oo-n-de-datos-del-INE-a-Fuerzas-y-Cuerpos-de-Seguridad-del-Estado.pdfhttps://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2014-0010_Cesi-oo-n-de-datos-del-INE-a-Fuerzas-y-Cuerpos-de-Seguridad-del-Estado.pdf

señalamos, el agente encubierto informático se infiltra para participar en canales de comunicación cerrados, podrían verse conculcados el derecho al secreto de las comunicaciones (art. 18.3 CE), el derecho a la intimidad (art. 18.1 CE) y el derecho a la autodeterminación informativa (18.4 CE). Puesto que el investigado, en el seno de unas comunicaciones privadas podrá facilitar datos personales, información relativa a sus relaciones afectivas, sexualidad, etc. porque, el canal cerrado de comunicación, justifica una expectativa de secreto.[25]

En definitiva, si no se cumplen ciertas garantías legales tales como la obtención de la correspondiente autorización judicial para la intromisión en los derechos mencionados o el consentimiento del titular de los mismos para tal injerencia, las pruebas dimanantes de la investigación criminal podrían vulnerar los derechos fundamentales, circunstancia que influirá en la capacidad de las mismas para invalidar la presunción de inocencia en el proceso penal.

Pues bien, tal y como dispone el tenor literal del art. 11.1 de la LOPJ en los procedimientos se respetarán las reglas de la buena fe y, **"no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales"**. La prueba obtenida produciendo la vulneración de derechos fundamentales es ilícita.

En primer lugar, partiendo de la premisa del art. 11.1 LOPJ, y de conformidad con la STS 320/2011, es imprescindible distinguir entre las pruebas originales nulas, las pruebas derivadas de éstas (directa o indirectamente) y, las pruebas independientes y autónomas de la prueba nula. Estas últimas "deben estimarse independientes jurídicamente por proceder de fuentes no contaminadas, como serían aquellas pruebas obtenidas fruto de otras vías de investigación tendentes a establecer el hecho en que se produjo la prueba prohibida*"*.

Por tanto, en cuanto a las pruebas independientes y autónomas de la prueba nula se consideran independientes jurídicamente de aquella y válidas para enervar la presunción de inocencia. Y, para las pruebas originales nulas, se aplicará la regla de la exclusión,

[25] Fernández López, M. (coord.). (2017). *Justicia penal y nuevas formas de delincuencia.* Valencia: Tirant Lo Blanch.

que implica que las mismas no podrán ser tenidas en cuenta por el juzgador a la hora de dictar sentencia.

Por otro lado, en relación con la capacidad de las pruebas derivadas de las pruebas nulas para enervar la presunción de inocencia, debe hacerse mención a la conexión de la antijuridicidad. Así pues, la doctrina jurisprudencial ha dictaminado en numerosas ocasiones que la ilicitud constitucional se extiende también a las pruebas derivadas si entre ellas y las anuladas por la vulneración existe también una conexión natural o causal, presupuesto para poder hablar de prueba derivada de otra ilícitamente obtenida. En principio, todo elemento probatorio que pretenda deducirse a partir de un hecho que vulnera un derecho fundamental estaría también incurso en la prohibición de valoración.

Sin embargo, en determinados supuestos se admite que dichas pruebas son independientes jurídicamente de la vulneración producida y, por tanto, válidas y capaces de enervar el principio de presunción de inocencia, tal y como reza la STS 228/2017 de 3 de abril. Señala la mencionada sentencia que "para establecer si se está ante un supuesto en que debe aplicarse la regla general que se ha referido o, por el contrario, nos encontramos ante alguna de las hipótesis que permiten excepcionarla, habrá que **delimitar si estas pruebas están vinculadas de modo directo a las que vulneraron el derecho fundamental sustantivo**."

La doctrina de la conexión de antijuridicidad, conforme dictamina la STS 511/2015 de 21 de junio, aminora el efecto anulatorio derivado de la infracción de la norma constitucional, de tal modo que la anulación de la prueba derivada no se genera únicamente de la conexión causal entre la ilícita y la derivada, sino que se requiere conexión jurídica entre ambas.

Para validar las pruebas derivadas y excluir así la conexión de antijuridicidad se utilizan criterios como el descubrimiento inevitable, la fuente independiente, la ponderación de intereses y, la autoincriminación del imputado en el plenario, entre otras (STS 228/2017 de 3 de abril), por lo que existe cierto margen de discrecionalidad por parte del juzgador para valorar la existencia de conexión de antijuridicidad.

En cuanto a la teoría del descubrimiento inevitable, la misma implica que, si la experiencia indica que las circunstancias hubieran llevado necesariamente al mismo

resultado, no es posible vincular causalmente la segunda prueba (la prueba derivada) a la anterior, porque en estos casos faltará la conexión de antijuridicidad.

Por otro lado, la autoincriminación del imputado en el plenario puede valorarse como prueba independiente que rompa el nexo de antijuridicidad derivado de la inconstitucionalidad de las pruebas obtenidas. Así, "a partir de las declaraciones, prestadas con conocimiento de la nulidad de las escuchas telefónicas, se produce la desconexión de antijuridicidad con la prueba ilícita" (STS 511/2015 de 21 de julio).

Tampoco habrá conexión de antijuridicidad, tal y como dispone la sentencia del Tribunal Supremo de 3 de abril antes referida, si los datos obtenidos con la vulneración del derecho fundamental se combinan con otros que no tengan la misma procedencia que aquellos obtenidos con la vulneración, ya que se trataría de una fuente de prueba independiente.

En definitiva, la regla general es que la prueba obtenida con vulneración de derechos fundamentales es nula, por tanto, no desplegará efectos en el proceso. Y, la prueba derivada de aquella también será nula salvo que no exista conexión jurídica entre ambas, es decir, que falte la conexión de antijuridicidad. Para romper la conexión de antijuridicidad la doctrina utiliza numerosos criterios como la confesión del acusado en el plenario.

3.1.5. La prueba pericial informática.

Como ya se aventuró, en ocasiones se requiere la intervención de personal cualificado, como los peritos informáticos, para otorgar validez a la información contenida en un dispositivo electrónico en el marco de un proceso judicial.

Para las pruebas electrónicas, la doctrina jurisprudencial exige la constatación de la existencia del hecho a través de periciales informáticas cuando aquellas sean contradichas, lo cual no implica que únicamente sea válida la prueba digital que haya sido confirmada por perito informático. Así, para las pruebas digitales aportadas por las partes, se estará a lo dispuesto en el artículo 326.1 de la LEC que dispone que "los

documentos privados harán prueba plena en el proceso en los términos del artículo 319, cuando su autenticidad no sea impugnada por parte de a quien perjudiquen."

Entonces, **la prueba pericial informática será indispensable para los supuestos en que se impugne la veracidad de la prueba digital aportada**, tal y como dispone el Tribunal Supremo en sentencia nº 224/2017 de 8 de marzo, así como cuando se requiera el acceso a la información contenida en un dispositivo y la misma haya sido encriptada o eliminada o, simplemente, cuando el acceso a dicha información sea difícil y se requiera por ello conocimientos técnicos.

Por lo expuesto, procede en este punto definir la prueba pericial informática como la prueba practicada por un perito con conocimientos especializados en la materia, que consiste en la emisión de un informe sobre unos hechos a través del cual aporta al juez conocimientos técnicos que éste no posee y, permitiéndole así valorar el objeto de la prueba.[26] Los hechos se prueban a través de datos que se encuentran en un sistema informático así como en dispositivos electrónicos. [27] La prueba pericial informática, por tanto, no consiste únicamente en una constatación de hechos, sino que requiere una valoración por parte del perito especializado que dilucide la veracidad, exactitud, inalterabilidad de los mismos.

A pesar de lo expuesto, cabe señalar que los datos informáticos pueden introducirse en el proceso a través de distintos medios probatorios y no necesariamente mediante la pericial informática: a través de documentos electrónicos, como podría ser un *pdf*.; a través de medios de prueba tradicionales como la documental, es el caso de la impresión en papel de una cadena de correos electrónicos; la testifical, por ejemplo interrogando a un tercero que fue testigo de una conversación de *Whatsapp* que mantuvieron otras personas, etc.

En definitiva, toda información de valor probatorio digital podrá aportarse como prueba en el marco de un proceso. Y, esta aportación podrá hacerse a través de los medios de prueba tradicionales, no obstante, cuando se impugne la autenticidad de la misma, será

[26] Carmelo LLopis, J. (2016). "Prueba electrónica y notariado" en *La prueba electrónica. Validez y eficacia procesal*. Recuperado de: http://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf

[27] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en*…Op. Cit.

necesario recurrir al informe emitido por un perito informático que dictamine sobre la exactitud, veracidad y origen del contenido de la misma.

3.2. Incorporación de la prueba al proceso penal.

El acto del juicio oral es el momento en que se practica la prueba en el proceso penal y siempre con observancia de los principios de publicidad, oralidad, inmediación y contradicción. Además, con respecto al principio de contradicción, cabe señalar que para dar cumplimiento al mismo, la prueba contenida en soportes técnicos se reproducirá en el acto del juicio oral.[28]

El hecho electrónico puede incorporarse al proceso a través de un documento tradicional, como por ejemplo un mensaje de *Whatsapp* impreso en papel o mediante la aportación del propio documento electrónico, como puede ser un pendrive o cualquier medio que permita el almacenamiento de datos. También podrá acreditarse el hecho a través de medios de prueba tradicionales como el interrogatorio de parte o de testigos, mediante la prueba pericial o incluso el reconocimiento judicial, es decir, el acceso directo del juez al contenido del soporte electrónico en que se halle el hecho mediante el visionado o la audición del mismo.[29]

3.2.1. Requisitos de acceso: necesidad, pertinencia y utilidad.

El artículo 299 de la LEC, contempla la posibilidad de que las partes, en el marco de un proceso, aporten pruebas digitales y las describe como "los medios de reproducción de la palabra, el sonido y la imagen, así como a los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*"*.

En numerosas ocasiones se rechazan estas pruebas 'modernas', pero tal rechazo no se produce por su falta de encaje en tal precepto sino por motivos relacionados con su ilicitud o pertinencia, pues una negativa a su admisión aduciendo a razones legales

[28] Abel Lluch, X. y Richard González, M. (2013) *Estudios sobre prueba penal*…Op. Cit.
[29] Ortuño Navalón, C. (2014) *La prueba electrónica ante los tribunales*. Valencia: Tirant lo Blanch.

podría ser incluso inconstitucional, a la luz del art. 24.2 CE, que otorga a los ciudadanos el derecho a utilizar todos los medios de prueba pertinentes para su defensa.[30]

La admisibilidad de la prueba es el resultado de un juicio hecho por el juez sobre las condiciones del medio o actividad probatoria propuestos para su admisión en el proceso. Deberá determinarse si tal material probatorio cumple los requisitos de pertinencia, utilidad y legalidad.[31] La prueba que pretenda ser incluida en el proceso ha de reunir necesariamente dichos requisitos, pues su incumplimiento será motivo de inadmisión de la misma.

La necesidad, de conformidad con el tenor literal del art. 281 apartados 3 y 4 LEC, implica que, con carácter general, no será necesario probar hechos sobre los que exista conformidad de las partes, así como tampoco será necesario probar hechos que sean notorios de manera general.

La pertinencia implica que ha de existir relación entre el hecho que pretende acreditarse mediante el concreto medio probatorio y los hechos objeto de controversia en el proceso, tal y como disponen los arts. 281.1 y 283.1 LEC.

En relación con la utilidad de la prueba, el apartado segundo del art. 283 LEC señala que aquellas que no puedan contribuir en ningún caso a esclarecer los hechos controvertidos, serán inútiles. Y, será inútil aquella prueba que, conforme a la experiencia, se pueda prever que no logrará el resultado pretendido.

El requisito de la legalidad de la prueba, que está regulado en el apartado tercero del artículo 283 LEC, implica que cuando se pretenda acreditar un hecho por medio de una actividad contraria a la ley, tal actividad quedará prohibida y será inadmisible como medio de prueba, puesto que constituirá una prueba ilegal.[32]

Sin embargo, la verificación por el juez del cumplimiento de los mencionados requisitos para la admisibilidad de la prueba electrónica plantea ciertos problemas en ocasiones,

---

30 Muñoz Sabaté, L. (2017) *Técnica probatoria*…Op. Cit.

31 Bueno de Mata, F. (2014) *Prueba electrónica y proceso 2.0.* Valencia: Tirant Lo Blanch.

32 Bueno de Mata, F. (2014) *Prueba electrónica*… Op. Cit.

motivo por el cual, autores como DE URBANO CASTRILLO, establecen una serie de puntos que han de observarse para la decisión sobre la admisibilidad: a) identificar el equipo del que procede el documento electrónico, b) verificar que el funcionamiento del equipo sea correcto, c) demostrar que como consecuencia de los datos introducidos en el equipo se ha producido el resultado, d) explicar la fiabilidad del proceso de registro y salida de los datos obrantes en el equipo y e) acreditar por otros medios quienes participaron en el procedimiento de elaboración del documento. El cumplimiento de lo señalado en los puntos expuestos, debido a su complejidad técnica, evidencia la necesidad en muchas ocasiones de aportar prueba pericial informática, [33] como expusimos en epígrafes anteriores.

Es necesario puntualizar que los criterios de los Juzgados y Tribunales al resolver sobre la admisión de una prueba deben ser, en principio, de la máxima amplitud y generosidad a la hora de medir el juicio constitucional de la pertinencia, máxime cuando se trata de medios de prueba propuestos por la defensa.

La constitucionalización del derecho a la prueba comporta la exigencia de efectuar una lectura de las normas procesales tendente a permitir la máxima actividad probatoria de las partes, siendo preferible el exceso en la admisión de pruebas a una postura restrictiva (*favor probatione*). En estos términos se pronuncia la doctrina del Tribunal Constitucional, la STC 10/2009 de 12 de enero considera que la legislación procesal criminal debe ser interpretada "sin desconocimiento ni obstáculos" al derecho fundamental a la prueba; y la STC 1/1992, de 13 de enero, afirma que ″la garantía del art. 24.2 del derecho a la defensa, consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el Juez o Tribunal y al haber sido constitucionalizado impone una nueva perspectiva y una sensibilidad mayor en relación con las normas procesales atinentes a ello, de suerte que deban los Tribunales de justicia proveer a la satisfacción de tal derecho, sin desconocerlo ni obstaculizarlo".

[33] Bueno de Mata, F. (2014) *Prueba electrónica…* Op. Cit.

3.2.2. Impugnación de la admisión o inadmisión.

El juez decidirá por medio de auto sobre la admisión o inadmisión de la prueba. En caso de inadmisión, ésta deberá estar motivada.

En relación con el recurso a interponer frente al auto de admisión o inadmisión de la prueba, en función del procedimiento en que nos encontremos, existen una serie de precisiones [34]:

Así, en el procedimiento ordinario, conforme al art. 659 LECrim, contra el auto que declare la admisión de las pruebas no cabe recurso, y contra el auto que declare la inadmisión cabrá protesta en aras a interponer en su debido tiempo el recurso de casación contra la sentencia por quebrantamiento de forma y garantías procesales, al haberse propuesto en tiempo y forma una diligencia que se considera pertinente.

En el procedimiento abreviado, tal y como dispone el art. 785 LECrim, no cabrá recurso contra los autos de inadmisión o admisión de pruebas, sin perjuicio de que la parte agraviada por la inadmisión reproduzca su petición al inicio de las sesiones del juicio oral. En ese momento, el juez resolverá tal solicitud y, si volviese a ser denegada, tampoco cabrá recurso, salvo protesta para interponer el correspondiente recurso contra la sentencia.

Y, en el procedimiento ante el Tribunal del Jurado se pronunciará sobre la admisión o inadmisión de las pruebas el Magistrado Presidente en el auto de hechos justiciables, conforme al art. 37 de la Ley Orgánica del Tribunal del Jurado, salvo si la prueba se hubiese propuesto al inicio del juicio oral, entonces resolverá en el juicio oral, tras oír a las partes, tal y como dispone el art. 45 del mismo texto legal. Tampoco cabrá, en este caso, recurso contra el auto de inadmisión o admisión, sin perjuicio de hacer constar por las partes su oposición en aras al posterior recurso contra la sentencia.

[34] Romero Pradas, I. (coord.) (2017) *La prueba. Tomo II: La prueba en el proceso penal***.** Valencia: Tirant Lo Blanch.

3.3. Valoración de la prueba.

El tenor literal del art. 741 LECrim postula el principio de la libre valoración de la prueba cuando dispone 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".

Así, la regla general para la valoración de la prueba electrónica es el sistema de libre valoración, conforme a las reglas de la sana crítica tal y como dispone el art. 384.3 LEC. Las reglas de la sana crítica se identifican con las máximas de experiencia, que pueden ser definidas como generalizaciones basadas en un cierto número de experiencias precedentes, considerando que la experiencia denota lo que suele ocurrir en casos análogos. [35]

Este sistema de libre valoración no implica total discrecionalidad judicial ya que tal valoración ha de estar motivada pues ha de explicarse por el juzgador porqué otorga o no credibilidad a un concreto medio probatorio y, preservar así, el derecho a la presunción de inocencia. [36] Así, lo que implica la libre valoración de la prueba o estimación en conciencia es la apreciación y valoración por parte del juzgador de la prueba incriminatoria con arreglo a criterios de lógica y razonabilidad. Las cuestiones que ha de tener en cuenta para efectuar tal valoración son: a) Deberá analizarse si existe prueba de cargo sometida a los principios de inmediación, contradicción, publicidad e igualdad; b) Realizar un 'juicio sobre la suficiencia' que implica que, de existir prueba de cargo, habrá de comprobar si la misma es capaz de desvirtuar la presunción de inocencia y; d) Deberá el juzgador motivar razonadamente el decaimiento de la presunción de inocencia. [37]

---

[35] Urbano Castrillo, E. de (2009) *La valoración de la prueba electrónica*. Valencia: Tirant Lo Blanch.
[36] Abel Lluch, X. *Valoración de los medios de prueba en el proceso civil*. Recuperado de: http://itemsweb.esade.edu/research/ipdp/valoracion-de-los-medios.pdf
[37] Romero Pradas, I. (coord.) (2017) *La prueba…* Op. Cit.

4. AUTENTICIDAD DE LA PRUEBA: INTEGRIDAD O EXACTITUD DE LA MISMA.

Como señalamos anteriormente, la información penal útil obrante en dispositivos electrónicos o alojada en servidores, podrá ser incorporada al proceso mediante los medios probatorios oportunos. Pero para garantizar que los datos obtenidos en los registros hechos a dichos dispositivos o servidores permanecen inalterados o que son exactamente los contenidos en los mismos, se precisa de una serie de garantías que desarrollaremos a continuación.

4.1. Sobre el clonado de los datos.

La primera de las mencionadas garantías, se refiere al proceso de clonado de la información. Una vez que se accede o se obtienen los datos del dispositivo, se procede al volcado o clonado de los mismos, que supone realizar una copia espejo o *bit a bit* de la información obrante en el mismo. Esta podrá hacerse en el mismo lugar en que se encuentra o en un momento posterior. Básicamente lo que se realiza es una copia física del contenido del mismo. Pero es mediante el *hash*, una función basada en algoritmos que otorga al contenido de un archivo un valor numérico, como se corrobora que los datos que se encontraban en el dispositivo original no han sido manipulados y, por tanto, son los mismos que los que se hallan en la copia. Mediante este procedimiento deberá originarse un original de los datos, una copia resultado del clonado que será sobre la cual se practicará la pericial informática, y una segunda copia para el titular de los datos, para el caso de que fuese necesario que el mismo continuase con la actividad que viniese ejerciendo.[38]

Esta segunda copia se contempla para los casos en los que el dispositivo se utiliza en el ámbito laboral o mercantil y, su incautación pudiera paralizar la actividad normal de la empresa así como producir perjuicios a la misma o a terceros ajenos al delito. El original, una vez hecha la copia o clonado, quedará precintado a disposición del juzgado

[38] Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en*…Op. Cit.

para que, en el caso de que se cuestionase en el seno del proceso sobre la autenticidad o exactitud de la copia, pudiera cotejarse la misma con el original. [39]

4.2. Sobre la presencia del Letrado de la Administración de Justicia durante la práctica del clonado o volcado de datos.

En segundo lugar, los registros efectuados deben ser documentados. Debe encargarse de tal función el Letrado de la Administración de Justicia levantando acta en la que se indique con precisión las operaciones practicadas y las personas intervinientes en el registro. [40] Cabe precisar que, en ocasiones, para asegurar la efectividad de la diligencia de entrada y registro, la entrada en el domicilio se podrá practicar sin la presencia inmediata del Letrado de la Administración de Justicia aunque, posteriormente, la Policía Judicial deberá comunicar al mismo en qué circunstancias se produjo la entrada, qué Agente intervino, así como los efectos intervenidos.[41]

En la mencionada acta, deberá reseñarse el IMEI del dispositivo, el número de serie del disco duro extraído (sin acceder a su contenido) y, de tratarse de portátiles, *tablets* o *pendrives*, se procederá a precintar los mismos. Ello es así en aras a preservar la cadena de custodia. En el material precintado firmará el Letrado de la Administración de Justicia con rotulador permanente, en custodia policial. La policía deberá solicitar al juzgado el desprecinto y volcado de la información que se harán en sede judicial y de la que también se levantará acta.[42]

También será necesaria la presencia del Letrado de la Administración de Justicia durante el desprecintado del dispositivo electrónico intervenido que se halla bajo custodia policial. [43]

[39] Martín Martín de la Escalera, A. "El Registro de dispositivos de almacenamiento masivo de la información"
[40] López Barajas Perea, I. (2017). "Nuevas Tecnologías aplicadas a la investigación penal… Op.Cit.
[41] Circular 3/2015 de 6 de octubre sobre buenas prácticas en materia de ejercicio de la Fe Pública en la investigación penal del Tribunal Superior de Justicia de Murcia.
[42] Circular 3/2015 de 6 de octubre sobre buenas prácticas en materia de ejercicio…Op. Cit.
[43] López Barja de Quiroga (2009). "La interceptación de las comunicaciones: jurisprudencia del Tribunal Supremo" en *Tratado de Derecho Procesal Penal,* Ed. Aranzadi.

Sin embargo, en cuanto a la presencia del mismo durante el volcado de datos, la misma no constituirá requisito de validez de las operaciones realizadas. Tal y como reza la STS 256/2008 de 14 de mayo, dicha presencia es inútil e innecesaria dado que el Letrado de la Administración de justicia no es experto técnico en dicha materia, y por ello no se requiere su presencia durante la práctica de la pericial informática.

En el mismo sentido resuelve la STS 1599/1999 de 15 de noviembre cuando dispone que "lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia*"*. Por lo que bastaría con la presencia del mismo durante la entrada y registro al lugar cerrado en que se halle el dispositivo, siendo dispensable durante el proceso de volcado de los datos que además, suele ser un proceso lento cuya duración puede alcanzar horas.

En definitiva y, en consonancia con la jurisprudencia analizada, la presencia del fedatario judicial durante el volcado de datos obrantes en dispositivos electrónicos no actúa como presupuesto de validez de su práctica.

4.3. Sobre la presencia del investigado o su letrado durante el desprecintado y volcado de los dispositivos electrónicos.

Otra garantía que prevé la Ley de Enjuiciamiento Criminal y que se adiciona a la analizada anteriormente, es la presencia del investigado y su letrado durante el desprecintado del dispositivo electrónico, tal y como se contempla en el artículo 476 del citado texto legal, a fin de que esta parte pueda comprobar que el precinto está intacto y que, por tanto, no ha sido alterado el contenido del dispositivo.

No obstante, a pesar de que el mencionado precepto contemple la posibilidad de que el investigado esté presente durante la práctica de tal diligencia, así como la posibilidad de que este pueda nombrar a un perito que comparezca a la misma, "tal presencia no

constituye presupuesto de validez de la diligencia" y así lo dispone la Audiencia Nacional en sentencia núm. 34/2014 de 24 de julio (en el mismo sentido resuelve la STS 187/2015 de 14 de abril). Por lo que la ausencia del investigado durante el desprecinto y acceso a la información contenida en el dispositivo electrónico, no invalida por sí misma la cadena de custodia y, por tanto, no desvirtúa la autenticidad de la prueba.

4.4. Sobre la cadena de custodia.

La observancia de las garantías descritas y analizadas en los puntos anteriores para asegurar la autenticidad de la prueba, es lo que constituye la cadena de custodia. Así, aunque la ley no codifica los requisitos de la cadena de custodia, en el art. 338 LECrim hace referencia a la misma cuando dispone que "los instrumentos **se recogerán de tal forma que se garantice su integridad** y el juez acordará, su retención, conservación o envío al organismo adecuado para su depósito."

En primer lugar, la cadena de custodia podría definirse, como reza la SJP Gijón 39/2016 de 6 de julio, como los actos de recogida, guarda y traslado de las evidencias obtenidas en el curso de la investigación criminal dirigidos a preservar y garantizar su autenticidad e indemnidad para poder ser utilizadas como prueba de cargo en el proceso penal. Y, a su vez, esta tiene relación con la prueba pericial cuando las evidencias son objeto de un posterior estudio técnico.

De forma más sencilla la define la STS 491/2016 de 8 de junio cuando dispone que "la cadena de custodia es el **proceso transcurrido entre que los agentes de la policía intervienen un efecto del delito que puede servir como prueba de cargo, hasta que se procede a su análisis, exposición o examen** en la instrucción o en el juicio". Por tanto, el fin de este proceso es garantizar que lo que se ha recogido y sobre lo que recaerá el juicio es lo mismo.

En definitiva, son numerosas las ocasiones en que la doctrina jurisprudencial se ha pronunciado sobre la cadena de custodia y ha definido la misma, el Tribunal Supremo en STS 6/2010 de 27 de enero, dictaminó que "la integridad de la cadena de custodia

garantiza que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y del juicio del tribunal es lo mismo."

Es de tal envergadura el papel que la cadena de custodia ejerce que, la ruptura de la misma, podría dar lugar a la vulneración del derecho a un proceso con todas las garantías. Esto es, una infracción relevante en la misma determinaría la invalidez de la prueba ya que comportaría la imposibilidad de asegurar la autenticidad de la misma.

En este sentido, el Tribunal Constitucional en sentencia núm. 170/2003 de 29 de septiembre para un supuesto en que los soportes informáticos incautados durante una entrada y registro no fueron correctamente identificados, sellados y precintados estima que se había "producido una deficiente custodia policial y control de dicho material" y que, por tanto, no podía garantizarse la inexistencia de eventuales manipulaciones o alteraciones del mismo habiéndose producido por la sentencia recurrida la vulneración a un proceso con todas las garantías.

Es preciso tener la certeza de que lo que se interviene y se traslada, para ser analizado y estudiado es lo mismo en todo momento. Y ello es así porque la ruptura de la cadena de custodia incide, sin lugar a duda, sobre la fiabilidad y autenticidad de la prueba tal y como dispone la STS 491/2016 de 8 de junio antes referida. Pero no basta con que, la parte que pretende alegar la ruptura de la cadena de custodia, haga "una simple reflexión genérica a cerca de los riesgos potenciales de adulteración ara desencadenar las dudas sobre su efectiva manipulación, con el consiguiente efecto en el ámbito del derecho a la presunción de inocencia", tal y como aduce la STS 287/2017 de 19 de abril, sino que la parte que pretenda hacer valer tal ruptura podrá proponer prueba pericial alternativa al dictamen ya elaborado por expertos y, podrá designar a un experto para que esté presente durante la pericial acordada por el Juez.

Una **infracción de escasa relevancia** de la cadena de custodia no determinaría por sí misma la exclusión de la prueba del proceso, "por lo que la misma debe igualmente ser valorada como prueba de cargo y", por tanto, "apta para desvirtuar la presunción de

inocencia, sin perjuicio de que el defecto apreciado pueda afectar a su poder de convicción o fiabilidad*"* (SJP Gijón 39/2016 de 6 de julio).

A pesar de que la regularidad de la cadena de custodia es un presupuesto para la valoración de la pieza de convicción ocupada, ya que es la única manera de garantizar que lo ocupado y lo que se analiza no ha sido alterado, "el incumplimiento de la misma no produce la nulidad de la prueba sino **que cuestiona su autenticidad**" y, es en función de la relevancia que ostente la infracción cometida como se determinará la posibilidad o no de que sea valorada como prueba de cargo (STS 1072/2012 de 11 de diciembre).

En conclusión, la cadena de custodia la conforman las medidas que han de adoptarse para garantizar la identidad e integridad de las evidencias obtenidas durante la investigación y garantizar así su total eficacia procesal. Su ruptura no permitiría afirmar la 'mismidad'[44] de la prueba y, en consonancia, podría desvirtuar la misma.

4.5. Manipulación de la prueba.

Hemos insistido a lo largo del presente trabajo en que la propia naturaleza de las pruebas digitales hace posible la manipulación de las mismas, por ejemplo, podrá manipularse un 'pantallazo' aportado en documento impreso bien suprimiendo o añadiendo partes a la conversación mantenida o bien porque esa conversación nunca tuvo lugar, pues el usuario creó una cuenta fingiendo una identidad y a través de la misma mantuvo una conversación consigo mismo. Pues bien, el que aporte en el seno de un proceso pruebas que ha manipulado para fundar sus alegaciones incurre en un delito de estafa procesal, si finalmente se dicta a su favor una resolución de fondo respecto a la cuestión planteada[45] que suponga un perjuicio económico ilícito para otro.

El delito de estafa procesal está regulado en el art. 250.1.7º del Código Penal, el citado precepto dispone que "incurren en la misma los que, en un procedimiento judicial de

[44] Concepto utilizado por la jurisprudencia en numerosas ocasiones para referirse a la inalterabilidad de la prueba (STS 575/2013 de 28 de junio, SAP Madrid 15/2012 de 3 de febrero).

[45] Díaz Morgado, C. (coord..) (2016) *Manual de Derecho Penal económico y de empresa. Parte general y parte especia*l. Valencia: Tirant Lo Blanch.

cualquier clase, manipularen las pruebas en que pretendieran fundar sus alegaciones o emplearen otro fraude procesal análogo, provocando error en el juez o tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero**."**

Se trata de una estafa común, con la diferencia de que, en esta ocasión, el sujeto pasivo engañado es el órgano judicial, aunque el perjudicado sea otro, es el juez el que es inducido a dictar una resolución errónea o injusta que de otro modo no hubiera dictado, en perjuicio de una de las partes o de un tercero.[46] En ocasiones se acepta que el engañado sea la parte contraria, y no el juez, si la realización de artimañas realizadas en el seno del procedimiento determinan un cambio en su voluntad, si por ejemplo se allana o desiste.[47]

5. CASO PRÁCTICO.

I. OBJETO DEL DICTAMEN.

El objeto del presente dictamen es dar respuesta a la consulta formulada por Don Juan Carlos, que está siendo investigado en el procedimiento nº 1589/2016 por los delitos del art. 172, 183 ter y, 189 del Código Penal.

II. ANTECEDENTES DE HECHO.

Primero.- Denuncia de la que traen causas las diligencias previas.

El 12/01/2016, Doña María Pérez (madre de la menor, Andrea Pérez Pérez) presentó denuncia ante la Policía por unas amenazas que su hija había sufrido por internet, los días 06/01/2016 y 12/01/2016. Las amenazas consistían en difundir un video de la menor desnuda y que habría sido grabado a través de una *webcam*.

---

[46] Encinar del Pozo, A. y Villegas García, A. (coords.) (2016). *Código Penal con jurisprudencia sistematizada*. Valencia: Tirant Lo Blanch.

[47] Díaz Morgado, C. (coord..) (2016) *Manual de Derecho Penal…* Op. Cit.

En ese momento se desconocía: 1) la identidad de la persona que realizaba las amenazas; 2) las direcciones de correo electrónico asociadas al usuario que realizaba las amenazas y; 3) la IP desde la que se conectaba este usuario.

La madre de la menor acompaña a la denuncia 'pantallazos' de las conversaciones mantenidas entre la menor y esa persona sin identificar, que habían tenido lugar en la red social *Facebook*.

Segundo.- Inicio de diligencias previas y sobreseimiento y archivo de las mismas.

El 13/01/2016, el Juzgado de Instrucción nº1 de Santa Cruz de Tenerife, incoó diligencias y, a continuación, declaró el sobreseimiento provisional y el archivo de las mismas por entender que no existían datos suficientes para conocer la identidad de los posibles responsables.

Tercero.- Solicitud de la policía dirigida al juzgado para el libramiento de un oficio a la compañía *Movistar* y a *Microsoft*.

En tal petición, la Policía dijo haber mantenido una entrevista con la menor, aun cuando no consta ningún extremo de la misma en el oficio. En dicha entrevista la menor habría señalado que los mensajes que recibía procedían de dos perfiles, de los cuales sólo podía aportar una serie de datos. Esos datos habrían sido, la ID y los datos completos de la cuenta *Facebook*.

La policía señaló que *"*se solicitó a la red social *Facebook* información sobre dichos perfiles al objeto de obtener datos que pudieran llevar al autor de estos hechos", así como las IPS de conexión de esos perfiles. Sin embargo, no se encuentra en las actuaciones el contenido de tal petición.

La documentación adjuntada en el oficio había sido remitida por *Facebook*, extramuros del ámbito judicial. Tal documentación fue obtenida durante el periodo en que las diligencias judiciales se habían archivado, esto es, se obtuvo sin autorización judicial.

La mencionada documentación, que habría sido facilitada por *Facebook,* consistía en:

1. **IPs** desde las que se conectaron los usuarios referidos por la madre de la menor.
2. **El contenido de todas las conversaciones mantenidas por el investigado con otras menores distintas de la denunciante** desde 29/11/2015 hasta el 25/01/2016.

Cuarto.- Ampliación de la denuncia hecha por la madre de la menor.

En las diligencias policiales 1589/2016 consta lo siguiente:

4.1. Que la madre de la menor amplió la denuncia el **24 de enero de 2016**, manifestando ante la Policía que a su hija le habían vuelto a remitir mensajes. Se dice que se aportan, pero no se encuentran en las actuaciones que tenemos.

4.2. Que la madre de la menor se presentó nuevamente en comisaria el **30 de marzo**, denunciando la existencia de nuevos mensajes amenazantes, lo que motivó que el Instructor de la Policía (no S.S.) citara, para ser oídas en declaración, a otras menores (Doña Verónica Martín y Doña Mónica Mena), que aparecían en las conversaciones inicialmente remitidas por *Facebook*.

4.3. Posteriormente, se tomó declaración a otra menor, Sara Rodríguez.

Quinto.- Entrada y registro en el domicilio del investigado.

5.1. El **10 de mayo de 2016**, la Policía remite oficio solicitando la entrada a domicilio. En esa petición de oficio se señala que: *"*Si por parte de V.I. tiene a bien conceder el Mandamiento de Entrada y Registro solicitado en el párrafo anterior, **esta diligencia se llevaría a cabo en la mañana del día 12 de mayo de 2016.***"*

5.2. El día **11 de mayo de 2016** se libra exhorto al Juzgado de Las Palmas de Gran Canaria para la entrada y registro, por ser éste el partido judicial donde radica el lugar del domicilio del investigado. Ese exhorto fue enviado por fax, desde el Juzgado de Santa Cruz de Tenerife al Juzgado de Las Palmas de Gran Canarias, a las **12:38 horas de ese día 11 de mayo**.

5.3. El **Auto acordando la entrada es del 12 de mayo,** pero no se especifica en el mismo cuándo ha de procederse a la entrada en el domicilio.
Sin embargo el testimonio del Auto de Entrada expedido por la Secretaria Judicial del Juzgado de Instrucción nº1 de Santa Cruz de Tenerife es del 11 de mayo de 2016.

5.4. La **Diligencia de Entrada y Registro tiene fecha de 11 de mayo** y se fija como fecha de inicio la de las **09:20 AM**.

5.5. En dicha entrada y registro se incauta el portátil del investigado y se visiona el contenido del mismo.

III. CUESTIONES PLANTEADAS.

De acuerdo con los antecedentes de hecho expuestos, se suscitan las siguientes cuestiones jurídicas:

3.1. Sobre el derecho al secreto de las comunicaciones y su posible vulneración.

Examinar si se ha producido una vulneración al secreto de las comunicaciones con el acceso a los chats de conversaciones mantenidas entre los menores, cuando esas conversaciones han sido facilitadas por una de las menores participantes en la conversación.

Análisis sobre si se ha producido vulneración al secreto de las comunicaciones con las conversaciones facilitadas por la red social *Facebook*.

3.2. Sobre la autenticidad de las conversaciones aportadas por la madre de la menor.

3.3. Determinar si los rastreos para localizar direcciones IP pueden realizarse sin autorización judicial.

3.4. Irregularidades en la entrada y registro practicada en el domicilio del investigado.

IV. NORMATIVA Y DOCTRINA APLICABLE.

Para la resolución de las cuestiones jurídicas planteadas en el apartado anterior, utilizaremos la siguiente normativa, doctrina y jurisprudencia:

Preceptos legales:

- Artículo 18.3 Constitución Española
- Artículo 18.1 Constitución Española
- Artículo 588 ter k) Ley de Enjuiciamiento Criminal
- Artículo 588 sexies a) Ley de Enjuiciamiento Criminal
- Artículo 338 Ley de Enjuiciamiento Criminal

Dictámenes y circulares de la Fiscalía General del Estado:

- Circular 1/2003 de la Fiscalía General del Estado
- Dictamen 1/2016 de la Fiscalía General del Estado

Jurisprudencia del Tribunal Constitucional:

- STC 170/2013 de 7 de octubre
- STC 56/2003 de 24 de marzo
- STC 98/2000 de 10 de abril
- STC 156/2001 de 2 de julio
- STC 130/200 de 29 de mayo

Jurisprudencia del Tribunal Supremo:

- STS 864/2015 de 10 de diciembre
- STS 300/2015 de 19 de mayo
- STS 786/2015 de 4 de diciembre

Jurisprudencia Audiencias Provinciales:

- SAP Santa Cruz de Tenerife 118/2017 de 4 de abril

V. FUNDAMENTOS JURÍDICOS.

5.1. Sobre el derecho al secreto de las comunicaciones y su posible vulneración.

En primer lugar, podemos definir el objeto de la protección del **derecho al secreto de las comunicaciones** (art. 18.3 CE), a la luz de lo señalado por el Tribunal Constitucional en la STC 170/2013, de 7 de octubre, como "el proceso de comunicación en libertad y no por sí solo el mensaje transmitido".

Señala la Fiscalía General del Estado, en la Circular 1/2003, que tal protección constitucional ampara todos los medios de comunicación conocidos así como aquellos que puedan aparecer en el futuro. Pues bien, en esta ocasión la posible vulneración se produce en una red social (*Facebook)*, por lo que, por medio de este moderno medio de comunicación, también será susceptible de vulneración el secreto de las comunicaciones.

Este derecho abarca todo el proceso de comunicación, el contenido del mensaje, la identidad de los interlocutores y datos del mismo como la duración del mensaje, el origen y destino, etc. Es evidente que mientras la conversación está teniendo lugar, opera la protección al secreto de las comunicaciones, sin embargo, cuando esta ha finalizado, se estima que el contenido del mensaje no está afecto al secreto de las comunicaciones, sin perjuicio de que pueda estar tutelado por el derecho a la intimidad.[48] Y, en este sentido se pronuncia la STC 56/2003, de 24 de marzo.

Teniendo en cuenta lo señalado y, **en relación con el acceso al contenido de los chats con otros menores distintos de la denunciante inicial**, no constituiría una vulneración al secreto de las comunicaciones pues, **quien lo aporta es uno de los comunicantes**. Y ello, pese a que tal aportación se realice sin consentimiento del resto de participantes en la comunicación. En este sentido se pronuncia la Sentencia del Tribunal Constitucional nº 56/2003, de 24 de marzo, cuando señala que quien graba una conversación con otro

[48] Delgado Martín J. (2016) Investigación tecnológica y… Op. Cit.

no vulnera tal precepto constitucional, así como tampoco quien durante una conversación telefónica emplea un aparato amplificador de la voz que permite que terceras personas presentes capten la conversación. Termina dictaminando la referida sentencia que "no existe vulneración del derecho al secreto de las comunicaciones pues es, precisamente, uno de los interlocutores en la comunicación telefónica quien autorizó expresamente a la Guardia Civil a que registrara sus conversaciones*"*. En el mismo sentido, STS 864/2015 de 10 de diciembre.

Además de lo anterior y, como apuntamos anteriormente, dado que la conversación ha finalizado, entendemos que no es susceptible de ser vulnerado el secreto de las comunicaciones en este concreto hecho.

Cuestión distinta es que con el visionado de conversaciones ya finalizadas y entregadas por uno de los participantes en la comunicación, la vulneración se haya producido del derecho a la intimidad (18.1 CE), definido por la STS 170/2013 como un derecho cuyo objeto es otorgar protección "a un ámbito reservado de la vida de las personas excluido del conocimiento de terceros en contra de su voluntad".

En cuanto a las **comunicaciones facilitadas por la red social *Facebook***, nada consta en las diligencias que nos permita pensar que tales comunicaciones han sido obtenidas con la correspondiente autorización judicial. Partimos, por tanto, de la base de que la policía requiere a *Facebook* para que le entregue determinadas conversaciones y *Facebook* procede a su entrega. En este caso concreto, las conversaciones entregadas ya tuvieron lugar, por lo que nos encontramos en el ámbito cuya protección ya no concierne al derecho al secreto de las comunicaciones sino al derecho a la intimidad.

Con respecto a este hecho, haremos alusión a la STS 865/2015, de 10 de diciembre, que dispone que la presunción de un fin legítimo, como la persecución de delitos, puede justificar una inmisión policial sin necesidad de autorización judicial previa. Dictamina la misma: "aunque el art. 18.1 CE no prevé expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad, su ámbito de protección puede ceder en aquellos casos en los que se constata la existencia de un interés constitucionalmente prevalente al interés de la persona en mantener la privacidad de determinada información". En el mismo sentido STC 98/2000, de 10 de abril y STC 156/2001 de 2 de julio.

5.2. Sobre la autenticidad de las conversaciones aportadas por la madre de la menor.

Por otra parte, interesaría impugnar la autenticidad de los 'pantallazos' de las conversaciones aportadas por la madre de la menor pues, la prueba de una comunicación bidireccional mediante sistemas de mensajería instantánea debe ser abordada con extremada cautela**.** "**La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas**. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido" (STS 300/2015, de 19 de mayo). Por tanto y, en consonancia con la resolución mencionada, si se impugnan los 'pantallazos' presentados y por ningún otro medio probatorio puede sustentarse el supuesto contenido de los mismos, no será prueba de cargo válida.

No obstante, debemos recordar que algunas menores han declarado –según la policía– en el mismo sentido que la menor de cuya denuncia traen causa las presentes diligencias. De no haber menores que declaren en este sentido, u otras pruebas que permitan dotar de veracidad los pantallazos aportados por la madre de la menor, será necesario la realización de una prueba pericial que acredite la existencia de la comunicación, su origen, destino y contenido. En este sentido se pronuncia el Dictamen 1/2016 de la Fiscalía General del Estado sobre valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas.[49]

[49] Dictamen 1/2016 de la Fiscalía General del Estado. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Dictamen%20nº%201-

5.3. Sobre la posibilidad de realizar rastreos sobre las direcciones IP sin autorización judicial.

La Circular de la Fiscalía General del Estado 1/2003, en cuanto a los rastreos para localizar direcciones IP, señala que éstos pueden realizarse sin necesidad de autorización judicial, ya que no se consideran datos confidenciales preservados al conocimiento público.

Tras la averiguación de la IP, las actuaciones posteriores de identificación y localización de quien sea la persona que tiene asignada dicha IP, si precisarán autorización judicial. En este sentido resuelve la SAP Santa Cruz de Tenerife 118/2017, de 4 de abril, cuando dispone que **"la necesidad de autorización judicial, se extiende a la cesión de datos que permitan la identificación del titular de la línea asociada a una dirección IP** específica que está accediendo a la red (la dirección IP es un número único e irrepetible con el cual se identifica un ordenador conectado a una red que usa el protocolo Internet Protocol). Tal exigencia legal se establece en el art. 588 ter k (identificación mediante número IP) según redacción dada por LO 13/2015 de 5 de octubre."

Además, y en relación con lo expuesto en el epígrafe anterior, la mencionada sentencia precisa que el rastreo de IP no afecta al secreto de las comunicaciones, si acaso, al derecho a la intimidad de manera leve que, por razones de orden público y, para la persecución de determinados hechos delictivos, es clara la habilitación policial para actuar.

Por tanto, no habría actuación reprochable si la misma se ha limitado al rastreo de una IP, pero del caso concreto y, de las actuaciones, se desprende que la actuación policial no se limitó al rastreo de la IP del investigado, sino que se obtuvieron datos que permitieron identificar al investigado como titular de la concreta dirección de IP.

2016%20sobre%20el%20valor%20probatorio%20de%20las%20capturas%20de%20pantallas.%20Unidad%20Criminalidad%20Informática.pdf?idFile=5838c1ef-1b11-49bf-92f4-066d003af630

5.4. Irregularidades en la entrada y registro practicada en el domicilio del investigado.

En primer lugar, el Auto que autorice la entrada y registro precisa de una serie de requisitos, pues es doctrina jurisprudencial consolidada (por ejemplo, la STC 130/2000, de 29 de mayo) que para que la motivación del Auto que autorice la entrada sea suficiente ha de tener un contenido mínimo consistente en un juicio de proporcionalidad entre la limitación que se impone al derecho fundamental restringido y su límite medida, la idoneidad y necesidad de la medida y el equilibrio entre el sacrificio sufrido por el derecho fundamental limitado y la ventaja que se obtendrá con tal limitación. Pero además, dispone la referida sentencia, "**el órgano jurisdiccional deberá precisar con detalle las circunstancias espaciales (ubicación del domicilio) y temporales (momento y plazo) de la entrada y registro** y, de ser posible, también las personales (titulares u ocupantes del domicilio en cuestión)".

Cabe poner de relieve, en este punto, la evidente contradicción que hay entre las fechas, pues el Auto que acuerda la entrada es del día 12 de mayo de 2016 y la diligencia de entrada se practica el día 11 del mismo mes, un día antes. Tampoco encajarían las horas en que suceden los hechos, pues, como ya señalamos, el fax remitiendo el exhorto al Juzgado de Instrucción de Las Palmas de Gran Canaria se habría enviado a las 12:38 horas de ese día 11 y la diligencia de entrada se habría producido, según consta en el Acta a las 09:20 horas. Por ello, entendemos que la entrada se produjo sin ningún tipo de habilitación judicial, en contravención con lo dispuesto en el art. 546 LECrim y tal infracción determinaría la nulidad de la diligencia practicada [50].

Por otra parte, y en el supuesto de que la entrada y registro se hubieran practicado con la correspondiente autorización, como consecuencia de la misma, se hallaron en el domicilio del investigado un ordenador portátil y un teléfono móvil, dispositivos electrónicos que fueron incautados. Lo habitual es que la resolución que autoriza la entrada y registro habilite también para incautar los dispositivos que se hallen en el mismo. En este sentido, la STS 786/2015, de 4 de diciembre señala que se hace

[50] Molina Pérez, T (2010) "La diligencia de entrada y registro practicada en la instrucción". Recuperado de: file:///Users/martaacosta/Downloads/Dialnet-LaDiligenciaDeEntradaYRegistroPracticadaEnLaInstru-3170491.pdf

extensiva la habilitación judicial para la intromisión domiciliaria a la aprehensión de todos los soportes de información que se hallen en la vivienda.

Sin embargo, la autorización de entrada y registro puede amparar la posterior aprehensión del dispositivo encontrado en la vivienda pero no así el visionado del contenido del mismo. Para tal visionado, se requerirá autorización judicial expresa en tal sentido, indicando las razones que legitiman el acceso por la policía a la información contenida en los dispositivos, tal y como dispone el art. 588 sexies, apartado a) LECrim.

En el supuesto que nos ocupa, la autorización judicial de entrada y registro nada disponía en relación con el acceso a los datos obrantes en los dispositivos, podría entenderse, conforme a la redacción del precepto mencionado, que ello vulnera las previsiones legales e invalidarse por ello el acceso a tal contenido. Sin embargo, hay jurisprudencia que entiende que, en caso de ausencia de autorización judicial, podrá ser visionado el contenido de los dispositivos electrónicos (ordenador portátil y móvil en este caso), siempre que tal visionado esté motivado por la concurrencia de otros bienes jurídicamente protegidos. Por lo que, esta actuación policial podría encontrar acomodo en este supuesto, si se alegase que el interés que se trataba de proteger era mayor que el derecho a la intimidad del acusado (STS 786/2015, de 4 de diciembre).

El visionado del material contenido en el teléfono móvil y en el ordenador portátil suscita otra serie de problemas, relativos esta vez a la garantía de la indemnidad o mismidad de lo hallado en tales dispositivos en el momento de la entrada y registro y, en un momento posterior, cuando se accede a su contenido por los agentes sin ningún tipo de garantías que permitan asegurar que no ha sido alterado el mismo.

Consideramos que se ha incumplido por los agentes lo dispuesto en el art. 338 LECrim, relativo a la cadena de custodia. Pues, en primer lugar, tuvo que procederse por el Letrado de la Administración de Justicia al levantamiento de acta en la que se indicase con precisión el IMEI del dispositivo móvil, el número de serie y la marca del ordenador portátil y posteriormente, practicarse el precintado de los mismos. Y, si quería accederse al contenido de los dispositivos, consideramos que debió hacerse previamente una copia o clonado de los mismos de forma que se hubiese garantizado la inalterabilidad del contenido hallado en los dispositivos.

Por lo expuesto, entendemos que se ha roto la cadena de custodia y que, de tenerse en cuenta estas pruebas y considerarse las mismas capaces para desvirtuar la presunción de inocencia, se podría vulnerar con ello el derecho a un proceso con todas las garantías.

VI. CONCLUSIONES.

I. No se ha vulnerado el derecho al secreto de las comunicaciones puesto que, en los dos casos analizados, los procesos de comunicación habían finalizado ya. En tales casos podría estimarse vulnerado el derecho a la intimidad, no obstante, teniendo presente que la doctrina jurisprudencial 'sacrifica' este derecho cuando concurre con otro interés constitucional relevante.

II. Cabría impugnar la autenticidad de los 'pantallazos' aportados por la madre de la menor en tanto no pueda acreditarse la validez de los mismos por otros medios de prueba y, teniendo en cuenta que, en todo caso, podría realizarse una pericial informática para comprobar la existencia de la comunicación.

III. La actuación de la policía sin autorización judicial no se limitó al rastreo de la IP del investigado, sino que se obtuvieron datos que permitieron identificar al investigado como titular de la concreta dirección de IP, en contravención de reiterada jurisprudencia.

IV. La autorización, posterior diligencia de entrada y registro adolecen de ciertas incongruencias que permiten concluir que la entrada y registro se practicaron sin habilitación judicial. Obviando la anterior premisa, debe señalarse que al incautarse y visionarse el contenido del ordenador portátil y del dispositivo móvil obtenidos en la entrada y registro sin la correcta observancia de las garantías legales, podría haberse quebrantado la cadena de custodia.

6. CONCLUSIONES.

PRIMERA. **SOBRE EL CONCEPTO DE PRUEBA DIGITAL.**

La primera conclusión a la que llegamos tras abordar el tema de "la prueba digital" es que, a pesar de que muchos autores han definido la misma, no hay un concepto legal dado por el legislador para la prueba digital, por lo que para definir la misma nos hemos remitido a las definiciones hechas por los autores que, en muchas ocasiones no son unánimes.

SEGUNDA. **SOBRE LA POSIBLE VULNERACIÓN DE DERECHOS FUNDAMENTALES EN LA FASE DE OBTENCIÓN DE LA PRUEBA DIGITAL.**

Dispone la jurisprudencia analizada que para una intromisión sin consentimiento en el domicilio o en el secreto de las comunicaciones, se requiere necesariamente autorización judicial. Sin embargo, para otras intromisiones que pudieran afectar no a los mencionados derechos sino a otros, como el derecho a la intimidad, establece que no necesariamente han de ser acordadas en todo caso por autoridades jurisdiccionales. Por lo cual, no es *constitucionalmente correcta la ecuación afectación de la intimidad-necesidad inexcusable de previa habilitación judicial* (STS 864/2015, de 10 de diciembre).

Partiendo de la anterior premisa, son numerosas las ocasiones en que la jurisprudencia, para un caso en que se ha producido una inmisión policial sin autorización judicial, estima que el derecho al secreto de las comunicaciones no ha sido quebrantado por no haber una conversación en curso, pues la misma ya tuvo lugar, para luego terminar señalando que, en todo caso, el derecho que pudiera haber sido quebrantado es el derecho a la intimidad y que, al hacer la ponderación entre los intereses en juego, éste siempre cede.

En definitiva, esta conclusión jurisprudencial podría dar lugar, en cuantiosas ocasiones, a que la policía actuase sin la correspondiente autorización judicial requerida para el visionado del contenido de los dispositivos electrónicos tras la aprehensión de los

mismos amparándose en que, si la conversación no está vigente en el momento en que se visiona el contenido del dispositivo electrónico no se estaría vulnerando el derecho al secreto de las comunicaciones (cuya intromisión precisa en todo caso de autorización judicial), sino el derecho a la intimidad (para cuya intromisión no se precisa necesariamente de autorización judicial).

TERCERA. SOBRE EL REGISTRO REMOTO DE LOS DISPOSITIVOS ELECTRÓNICOS.

Hemos señalado que la obtención de la prueba digital podrá hacerse a través de la utilización de la figura del agente encubierto, a través de la incautación del dispositivo electrónico y, sin necesidad de aprehender el mismo, a través del registro remoto del dispositivo electrónico. Este último supuesto plantea ciertos problemas relativos a la acreditación de que el registro se ha producido desde que se dictó la resolución judicial que autorizaba el mismo y no antes de tal resolución.

Además, otro problema que plantea la utilización del registro remoto para la obtención de la información obrante en un dispositivo lo constituye dilucidar si aquello que prueba la comisión del hecho delictivo ha sido consecuencia de la conducta del investigado o si, por el contrario, ha sido manipulado por el agente encargado de la ejecución del registro remoto, pues no contamos con medidas que garanticen estos extremos.

CUARTA. SOBRE LA PERICIAL INFORMÁTICA.

Cuando el hecho que se acredita en la prueba digital sea contradicho, si se cuenta con otros medios de prueba que corroboren dicho hecho, como el testimonio de quién visionó los archivos de pornografía infantil que obraban en el ordenador del investigado o las conversaciones aportadas por la policía que mantuvo el investigado con usuarios de un foro de pornografía infantil en las que revelaba que disponía de tales materiales, no será precisa la realización de una pericial sobre la prueba digital que evidencia el hecho delictivo.

Sin embargo, cuando la única prueba con la que se cuenta es la digital y, su autenticidad es impugnada por la parte contraria nos encontramos ante una verdadera encrucijada,

pues como hemos expuesto a lo largo del presente trabajo, en estos casos se requiere la realización de una pericial informática, cuestión que, para quien no puede asumir los costes de la realización de un informe pericial que dictamine sobre la veracidad de la misma, impedirá que sus pretensiones lleguen a buen fin en el marco de un proceso.

QUINTA. SOBRE LA AUTENTICIDAD DE LA PRUEBA. LA CADENA DE CUSTODIA.

5.1. Sobre la aptitud para desvirtuar la presunción de inocencia dada por la jurisprudencia, en ocasiones, a elementos cuya custodia ha sido cuestionable.

A pesar de que las pruebas han de recogerse de tal forma que se garantice su integridad e inalterabilidad desde la recogida hasta su análisis, no son pocas las ocasiones en que la jurisprudencia ha otorgado valor de prueba de cargo y, por tanto, con aptitud para desvirtuar la presunción de inocencia, a pruebas cuya custodia ha sido deficiente por no haber sido preservada íntegramente la cadena de custodia. Un ejemplo de ello, lo constituye el hecho de que en la jurisprudencia analizada, por un lado se estime quebrantada la cadena de custodia por no ser los elementos objeto de análisis correctamente precintados y, por otro lado, que la presencia del investigado o su letrado durante el desprecintado de los mismos, no constituya presupuesto de validez de la diligencia. Pues entendemos que difícilmente podría alegarse el quebrantamiento de la cadena de custodia si no se permitiese en todo caso la presencia de, como mínimo, el letrado del investigado durante tal diligencia ya que, de no ser así, no podría corroborar el estado en que se encuentran los elementos incautados, que no se haya procedido a su manipulación o apertura con carácter previo a la realización de la pericial informática, etc.

5.2. Sobre la necesidad de utilización estricta de protocolos para garantizar la cadena de custodia.

A pesar de que existen garantías técnicas y protocolos para la recopilación, conservación, depósito, etc. de evidencias por parte de la policía, es imprescindible el cumplimiento escrupuloso por parte de la misma de dichas formalidades, pues como señalamos en el apartado anterior, entraña cierta dificultad probar la alteración o

quebrantamiento de la cadena de custodia. Además de que entra en juego el derecho fundamental del investigado a un proceso con todas las garantías, cuestión que no merece ser obviada.

Quizás se lograse la observancia de dichas garantías técnicas premiando y promoviendo la utilización de normas para la recopilación de evidencias que den indicaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales.

7. BIBLIOGRAFÍA Y JURISPRUDENCIA ANALIZADA.

Bibliografía.

- Abel Lluch, X y Richard González, M (2013) *Estudios sobre prueba penal*. Madrid: Wolters Kluwer.
- Abel Lluch, X. *Valoración de los medios de prueba en el proceso civil*. Recuperado de: http://itemsweb.esade.edu/research/ipdp/valoracion-de-los-medios.pdf
- Bueno de Mata, F (2012). *El Agente cubierto en internet: mentiras virtuales para alcanzar la justicia*. Recuperado de: https://dialnet.unirioja.es/servlet/articulo;jsessionid=4A7CF70253AEF84F98D8F7F8C4BCD955.dialnet01?codigo=4036206
- Bueno de Mata, F. (2014) *Prueba electrónica y proceso 2.0.* Valencia: Tirant Lo Blanch.
- Bueno de Mata. F. (2015) "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica" Nº 8627, Diario La Ley
- Carmelo LLopis, J. (2016). "Prueba electrónica y notariado" en *La prueba electrónica. Validez y eficacia procesal*. Recuperado de: http://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf
- Carnelutti, F (1982) *La prueba civil*. Buenos Aires: Depalma.
- Carrasco Mayans, S. (2016) "La alegalidad o limbo legal de la prueba electrónica" en *La prueba electrónica: validez y eficacia procesal*. Recuperado de: http://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf
- Delgado Martín, J. (2013) "La prueba electrónica en el proceso penal". *Diario La Ley*, Sección Doctrina. La Ley. Recurso electrónico: http://diariolaley.laley.es/home/DT0000245602/20170411/La-prueba-digital-Concepto-clases-y-aportacion-al-proceso
- Delgado Martín, J. (2016) *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: Wolters Kluwer.

- Díaz Morgado, C. (coord..) (2016) *Manual de Derecho Penal económico y de empresa. Parte general y parte especia*l. Valencia: Tirant Lo Blanch.
- Encinar del Pozo, A. y Villegas García, A. (coords.) (2016). *Código Penal con jurisprudencia sistematizada*. Valencia: Tirant Lo Blanch.
- Fernández López, M. (coord.). (2017). *Justicia penal y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch.
- García Torres, M. (2011). "La tramitación electrónica de los procedimientos judiciales, según la Ley 18/2011, de 5 de junio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil." Recuperado de: https://dialnet.unirioja.es/descarga/articulo/4405667.pdf
- Gil Antón, A. (2015). "El menor y la tutela de su entorno virtual a la luz de la reforma del Código Penal LO 1/2015" en Revista de Derecho UNED nº16/2015. Recuperado de: http://e-spacio.uned.es/fez/eserv/bibliuned:RDUNED-2015-16-7070/menor_y_tutela.pdf
- Gutiérrez Romero, F. (2016) "Algunas claves dela reforma de la Ley de Enjuiciamiento Criminal" Revista Aranzadi, nº 2/2016.
- López Barajas Perea, I. (2017). "Nuevas Tecnologías aplicadas a la investigación penal: el registro de equipos informáticos" en *Revista de Internet, Derecho y Política*. Recuperado de: http://www.redalyc.org/articulo.oa?id=78850913006
- López Barja de Quiroga (2009). "La interceptación de las comunicaciones: jurisprudencia del Tribunal Supremo" en *Tratado de Derecho Procesal Penal,* Ed. Aranzadi.
- Martín Martín de la Escalera, A. "El Registro de dispositivos de almacenamiento masivo de la información"
- Mata Barranco, N. de la "El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual" Revista Electrónica de Ciencia Penal y Criminología. Recuperado de: http://criminet.ugr.es/recpc/19/recpc19-10.pdf
- Molina Pérez, T (2010) "La diligencia de entrada y registro practicada en la instrucción". Recuperado de: file:///Users/martaacosta/Downloads/Dialnet-LaDiligenciaDeEntradaYRegistroPracticadaEnLaInstru-3170491.pdf

- Muñoz Sabaté, L (2017) *Técnica probatoria. Estudios sobre las dificultades de la prueba en el proceso*. Madrid: Wolster Kluwer.
- Ordoñez Solís, D. (2014) *La protección judicial de los derechos en internet en la jurisprudencia europea*. Madrid: Reus.
- Ortuño Navalón, C. (2014) *La prueba electrónica ante los tribunales*. Valencia: Tirant lo Blanch.
- Romero Pradas, I. (coord.) (2017) *La prueba. Tomo II: La prueba en el proceso penal*. Valencia: Tirant Lo Blanch.
- Urbano Castrillo, E. de (2009) *La valoración de la prueba electrónica*. Valencia: Tirant Lo Blanch.
- Valverde Mejías, R. *Cuestiones procesales relativas a la investigación de los delitos en red*. Fiscalía General del Estado. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Sr.%20VALVERDE.pdf?idFile=98ee6878-f370-403a-911b-7d71200a932a.
- Vela Mouriz, A. "Las 10 claves de la modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica." Wolters Kluwer. Recuperado de: http://pdfs.wke.es/4/8/8/0/pd0000104880.pdf

Enlaces Web:

- Circular 3/2015 de 6 de octubre sobre buenas prácticas en materia de ejercicio de la Fe Pública en la investigación penal del Tribunal Superior de Justicia de Murcia. Recuperado de: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunales-Superiores-de-Justicia/TSJ-Region-de-Murcia/Actividad-del-TSJ-Region-de-Murcia/Otros-documentos/Circulares/Circular-SG-TSJ-MU-3-2015--de-6-de-octubre--sobre-buenas-practicas-en-materia-de-ejercicio-de-la-Fe-Publica-en-la-investigacion-penal
- Dictamen 1/2016 de la Fiscalía General del Estado. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Dictamen%20nº%201-2016%20sobre%20el%20valor%20probatorio%20de%20las%20capturas%20de%20pantallas.%20Unidad%20Criminalidad%20Informática.pdf?idFile=5838c1ef-1b11-49bf-92f4-066d003af630

- Informe sobre la petición formulada por la Agencia Estatal de la Administración Tributaria para que se remita a dicha Agencia información con trascendencia tributaria obrante en los órganos jurisdiccionales. Del gabinete técnico del CGPJ. Recuperado de: http://daascompliance.es/wp-content/uploads/2017/09/Acuerdo-CGPJ-20-7-2017.pdf
- Informe nº10/2014 del gabinete jurídico de la Agencia Española de Protección de Datos. Recuperado de: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2014-0010_Cesi-oo-n-de-datos-del-INE-a-Fuerzas-y-Cuerpos-de-Seguridad-del-Estado.pdfhttps://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2014-0010_Cesi-oo-n-de-datos-del-INE-a-Fuerzas-y-Cuerpos-de-Seguridad-del-Estado.pdf
- Ministerio del Interior: "Estudio sobre la cibercriminalidad en España." Recuperado de: http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf

Jurisprudencia.

Tribunal Supremo:

- STS 224/2017, de 8 de marzo
- STS 163/2015, de 24 de marzo
- STS 404/2016, de 11 de mayo
- STS 786/2015, de 4 de diciembre
- STS 864/2015, de 10 de diciembre
- STS 320/2011, de 22 de abril
- STS 228/2017, de 3 de abril
- STS 511/2015, de 21 de junio
- STS 224/2017, de 8 de marzo
- STS 256/2008, de 14 de mayo
- STS 1599/1999, de 15 de noviembre
- STS 187/2015, de 14 de abril

- STS 491/2016, de 8 de junio
- STS 6/2010, de 27 de enero
- STS 491/2016, de 8 de junio
- STS 287/2017, de 19 de abril
- STS 1072/2012, de 11 de diciembre
- STS 300/2015, de 19 de mayo
- STS 575/2013, de 28 de junio

Tribunal Constitucional:

- STC 83/2002, de 22 de abril
- STC 170/2013, de 7 de octubre
- STC 199/2013, de 5 de diciembre
- STC 10/2009, de 12 de enero
- STC 1/1992, de 13 de enero
- STC 170/2003, de 29 de septiembre
- STC 56/2003, de 24 de marzo
- STC 98/2000, de 10 de abril
- STC 156/2001, de 2 de julio
- STC 130/2000 , de 29 de mayo

Audiencia Nacional:

- Sentencia Audiencia Nacional 3/2017, de 7 de febrero
- Sentencia Audiencia Nacional 34/2014, de 24 de julio

Audiencia Provincial:

- SAP Santa Cruz de Tenerife 118/2017, de 4 de abril
- SAP Madrid 15/2012, de 3 de febrero
- Auto AP Barcelona 95/2017, de 13 de febrero

Juzgado de lo Penal:

- SJP Gijón 39/2016, de 6 de julio