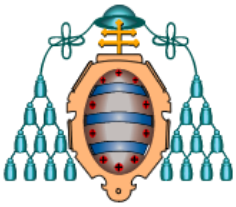
TRABAJO FIN DE MASTER

CURSO 2013/2014

MASTER UNIVERSITARIO EN ABOGACÍA

MEDIOS DE PRUEBA Y NUEVAS TECNOLOGÍAS



UNIVERSIDAD DE OVIEDO

MAYO 2014

ALUMNA: PATRICIA DÍAZ DÍAZ

TUTOR: JAVIER G. FERNÁNDEZ TERUELO

ÍNDICE DE CONTENIDOS

1. LA PROBLEMÁTICA DE LAS NUEVAS TECNOLOGÍAS COMO PRUEBA

1.1. ASPECTOS PREVIOS

La aplicación de las Nuevas Tecnologías a los medios probatorios es una realidad tan presente como escasamente regulada, quizá debido a la brusca irrupción de nuevas formas de comunicación como son las redes sociales Facebook o Twitter, así como por su carácter efímero o su rápida y fácil sustitución por nuevos medios; baste recordar cómo los SMS (*Short Message Service* o mensajes cortos) quedaron obsoletos y desplazados por la aplicación de mensajería multiplataforma (Whatsapp, Line, Telegram) en un breve lapso de tiempo. A todo lo anterior, habría que añadir que una de las notas características de este tipo de pruebas, su volatilidad y las infinitas posibilidades de manipulación y tratamiento. Por todo ello, entre otros motivos, resultaría imposible que el legislador hubiera podido prever una regulación legal respecto a su aportación al proceso, aunque mayor problema supone la comisión de delitos a través de estos medios, o incluso la aparición de nuevas modalidades comisivas.

A pesar de la imposibilidad legislativa de dar una respuesta jurídica rápida y eficaz a los problemas derivados del empleo masivo de la tecnología e Internet, también hay un claro intento de adaptación a esta realidad, y así cada vez existe una mayor especialización en la investigación policial de estos delitos, creándose unidades especializadas en el Cuerpo Nacional de Policía así como en La Guardia Civil, ya desde los años 90, que fueron creciendo a la vez que se popularizaba el acceso a Internet y proliferaban las conductas delictivas vinculadas a este medio. Como señala FERNÁNDEZ TERUELO[1], entre las conductas susceptibles de comisión a través de Internet destacan las relativas a la distribución de pornografía infantil, los daños informáticos, los atentados contra la propiedad intelectual o contra la intimidad, y junto a ellos, Internet se ha convertido en un medio muy útil para quienes desean realizar conductas fraudulentas que determinan un perjuicio económico a terceros, pudiendo ser consideradas formas típicas de estafa común o estafa informática. Pese a que la mayoría de las conductas desarrolladas a través de Internet no sean en esencia algo nuevo, la peculiaridad del medio les dota de una especial estructura que ha obligado a la constante especialización de determinados tipos delictivos. Es precisamente esa ruptura con algunos esquemas lo que ha ido determinando la ineficacia de ciertas figuras típicas, factor que ha estimulado, no siempre de forma exitosa, las tareas de modificación legislativa.

[1] FERNÁNDEZ TERUELO, J.G. "*Derecho penal e Internet*". Lex Nova, Valladolid 2011, (pp. 5 a 7).

1.2. LA PLURALIDAD TERMINOLÓGICA

Uno de los primeros problemas relacionados con las Nuevas Tecnologías es la falta de un término universal, utilizándose mayoritariamente el acrónimo TIC "Tecnologías de la Información y la Comunicación", especialmente desde la popularización del acceso a Internet, para referirse a las Nuevas Tecnologías (NNTT), término usado al comienzo de la irrupción de la tecnología, o incluso fundiéndose ambas en NTIC (Nuevas Tecnologías de la Información y la Comunicación).

Tampoco el término que describe la prueba que se obtiene de fuentes informáticas, es pacífico, utilizándose en ocasiones traducciones de vocablos provenientes de otras culturas jurídicas; así se emplea indistintamente evidencia digital, informática forense, prueba electrónica, prueba informática, prueba tecnológica, prueba audiovisual, prueba digital… ANGUAS BALSERA[2] propone unificar toda la nomenclatura empleada en la expresión "prueba informática", dado que existen tecnologías emergentes que ya no se basan en la electrónica, al menos en lo referido al cómputo o almacenamiento de la información, y por otro lado, términos como "electrónica" o "digital" no coinciden con la disciplina de cuyo objeto son estudio, que sí sería la Informática. En cambio, ABEL LLUCH[3] propone el uso del término "prueba electrónica", por su brevedad expresiva y porque alude a una realidad intangible en la que interviene la electrónica; asimismo, comparte un concepto amplio de documento que englobe tanto los presentados en soporte papel y firma manuscrita, cuanto en soporte distinto como audiovisual, informático o digital.

1.3. LA ELECCIÓN DEL MEDIO DE PRUEBA ADECUADO

La peculiaridad de los equipos informáticos o electrónicos a efectos probatorios es que el continente en sí mismo tiene escasa importancia, siendo la información que contienen sus archivos lo verdaderamente relevante, aunque admite excepciones, como en los casos en los que el objeto del delito es el propio equipo informático que ha sido sustraído o cuando, a falta de otras pruebas, las huellas de una persona en material informático pueden ser pruebas indiciarias de la autoría de lo contenido[4].

---

[2] ANGUAS BALSERA,J. *"La prueba informática: evolución, estado actual y propuesta de formalización" ,*en ABEL LLUCH, X. PICÓ I JUNOY, J. RICHARD GONZALEZ, M. (coords.) *"La prueba judicial, desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa"*. La Ley, Madrid 2011, (pp. 418 y 419).

[3] ABEL LLUCH, X., *"Nuevas Tecnologías y acceso al proceso"*, en ABEL LLUCH, X. PICÓ I JUNOY, J. RICHARD GONZALEZ, M. (coords.) *"La prueba judicial, desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa"*, op. cit., (pp. 345 y 346).

[4] STS 1281/2006 de 27 diciembre.

Como señala DE JORGE MESAS[5], a diferencia de otros medios de prueba, los útiles informáticos no mantienen una relación unívoca con un sólo medio probatorio, sino que la información que contienen puede incorporarse al proceso a través de distintos medios, siendo lo más frecuente proponerla como prueba documental. Cada medio tiene sus ventajas e inconvenientes, así, el reconocimiento judicial puede ayudar a formar una mayor convicción en el juez, pero también los archivos informáticos pueden dañarse o no funcionar el equipo informático correctamente. Por el contrario, los documentos impresos aportan mayor facilidad al poder leerse directamente, aunque el problema que presentan es acreditar su autenticidad.

1.4. LA AUTENTICIDAD E INTEGRIDAD DE LA FUENTE PROBATORIA

Es lo que se conoce como «Doctrina de la cadena de custodia». Como señala la STS 115/2014 de 25 de febrero *«el problema que plantea la cadena de custodia[6] es garantizar 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 el juicio de los juzgadores, es lo mismo. Es a través de la cadena de custodia como se satisface la garantía de la mismidad de la prueba»*. Se ha mantenido también por la doctrina que *«la cadena de custodia es una figura tomada de la realidad a la que tiñe de valor jurídico con el fin de, en su caso, identificar el objeto intervenido, pues al tener que pasar por distintos lugares para que se verifiquen los correspondientes exámenes, es necesario tener la seguridad de que lo que se traslada y analiza es lo mismo en todo momento, desde el momento en que se interviene hasta el momento final que se estudia y analiza y, en su caso, se destruye. Es el conjunto de medidas que se deben adoptar a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para garantizar así su total eficacia procesal[7]».*

La STS 303/2014 de 4 de abril recoge los criterios jurisprudenciales generales al respecto, que a modo de resumen, son las siguientes:

---

[5] DE JORGE MESAS, L.F. en su artículo *"La incorporación de las nueva tecnologías informáticas y de telecomunicaciones al proceso penal"* en VELASCO NUÑEZ, E. (coord.) *"Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia"*. Cuadernos de Derecho Judicial. Consejo General del Poder Judicial, Escuela Judicial, Madrid 2007, (pp. 358 a 365).

[6] SSTS 6/2010 de 27 de enero, 776/2011 de 26 de julio, 347/2012 de 25 de abril y 773/2013 de 22 de octubre.

[7] SAP de Huelva (Sección 3ª) de 22 de junio de 2012.

a) Se define como *«el conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba».*

b) 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 el juicio del tribunal es lo mismo. La regularidad de la cadena de custodia es un presupuesto para la valoración de la pieza o elemento de convicción intervenido; se asegura de esa forma que lo que se analiza es justamente lo ocupado y que no ha sufrido alteración alguna[8].

c) Respecto a la ruptura de la cadena de custodia, sus efectos repercuten sobre la fiabilidad y autenticidad de las pruebas[9], pudiendo tener una indudable influencia en la vulneración de los derechos a un proceso con todas las garantías y a la presunción de inocencia.

d) Asimismo señala el problema que supone que la LEC no contenga una regulación unitaria y sistemática sobre los requisitos y garantías de la cadena de custodia, si bien regula de forma dispersa algunos aspectos concretos sobre la materia, como los artículos 326, 334, 282, 292, 330, 338, 770.3 y 796.1.6 LECrim.

Dos ejemplos de análisis de la cadena de custodia de medios informáticos o electrónicos, son los siguientes:

1. La SAP de Málaga (sección 7ª, Melilla) 19/2013 de 21 de marzo, no aprecia ruptura en la **cadena de custodia de un Iphone**, por los siguientes motivos: El acusado entregó voluntariamente el teléfono móvil a la Guardia Civil; una vez en poder de los agentes, se comprobó que el teléfono estaba perfectamente identificado, con su marca, modelo y especialmente número IMEI *(International Mobile Equipment Identity)*, es decir, identidad internacional de equipo móvil, que es un número de serie, compuesto por quince dígitos, grabado en todos los dispositivos móviles, único para cada uno de ellos. Posteriormente fue analizado, en primer lugar por el Servicio de Información de la Guardia Civil de la Comandancia de Melilla, y luego por el Departamento de Análisis Forense, del Grupo de

[8] STS 1072/2012, de 11 de diciembre.

[9] STS 1029/2013, de 28 de diciembre.

Ciberterrorismo, de la Jefatura de Información de la Guardia Civil. Se concluyó que el dispositivo analizado era un iPhone de la marca Apple, modelo 4S con número de IME NUM010, con una tarjeta SIM de la compañía Orange, que tenía asociado el número de línea de teléfono NUM011. El dispositivo móvil, además de estar perfectamente identificado, en ningún momento estuvo fuera del control y custodia de la Guardia Civil ni del Juzgado instructor, que informó de todo lo relativo a dicho vestigio relacionado con el delito, acordando la devolución del teléfono móvil intervenido a su propietario una vez que se hubieran concluido las pruebas y/o análisis. Por todos estos motivos, no se apreció ruptura de la cadena de custodia.

2. La SAP de Murcia, Sección 3ª, 85/2011 de 25 de octubre, analiza la **cadena de custodia del disco duro de la CPU**[10] en un delito de corrupción de menores mediante pornografía infantil, estableciendo que la cadena de custodia del disco duro de la CPU del acusado hallado en su domicilio, se ha observado con todo rigor, por los siguientes motivos: El ordenador fue precintado al finalizar la diligencia, con autorización del Secretario Judicial, presente en el registro, que también autorizó su posterior traslado y depósito, a la Jefatura de Policía. Posteriormente se procede al desprecinto a presencia judicial y del Secretario, que da fe de dicha operación, del contenido, examen de carpetas, y clonación, previo traslado al Juzgado Instructor del mismo ordenador intervenido, para realizar el volcado del disco duro, acreditándose que se trata del que previamente había sido precintado, sellado y depositado en Jefatura con autorización del Secretario Judicial, conectando para ello el disco duro intervenido, precintado y sellado, a otro disco duro para obtener una copia idéntica, sobre la que realizar la prueba pericial, hallándose presente el Letrado defensor del imputado al momento del desprecinto y clonación del disco duro, que mostró su disconformidad respecto del número de serie del ordenador, a pesar de la intervención de la fe pública judicial en todas las operaciones realizadas sobre el mismo desde la entrada y registro hasta el volcado y clonación del disco duro a peritar, permaneciendo el original en sede judicial. Por último, en la prueba pericial practicada por la Policía Científica, fue examinado el disco duro obtenido, y el contenido de los soportes y carpetas halladas, la estructura de los directorios, y en el software instalado en el disco duro, se analizaron los programas, procediéndose al análisis de los archivos de pornografía infantil compartidos a través del Emule, y a la búsqueda de palabras claves utilizadas conocidas en el mundo de la pedofilia y claves y variaciones en el número. Capturando las pantallas en el Anexo del informe pericial.

[10] Acrónimo de Central Processing Unit, unidad central de procesamiento. Es el principal componente de un equipo informático.

1.5. LA INVESTIGACIÓN DE DELITOS EN INTERNET Y LA OBTENCIÓN DE LA PRUEBA

1.5.1. Cuerpo Nacional de Policía

A mediados de los años 90, se crearon unidades especializadas, coincidiendo con el auge y popularización de la informática y del acceso a Internet. En la actualidad su estructura orgánica se recoge en la Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía, que recoge en su Preámbulo: *«El conocido auge de las Tecnologías de la Información y las Comunicaciones (TIC) ha originado la creación de un espacio virtual en el que se realizan múltiples actividades, que afectan a la privacidad de las personas pero que también, en numerosos casos, produce efectos de distinta naturaleza jurídica, susceptibles de vulnerar la legalidad vigente utilizando estos medios por parte de personas que, amparadas en el anonimato, están dispuestas a obtener importantes beneficios mediante actividades ilícitas, aprovechando las posibilidades que ofrecen estas Tecnologías. Así, la mayoría de los delitos encuentran en estos medios un nuevo escenario, en una larga lista que es ocioso enumerar, ya que cada día aparecen nuevas formas de transgredir las leyes, tanto penales como administrativas. La delincuencia organizada en la Red, nos obliga por consiguiente a reforzar la presencia del Cuerpo Nacional de Policía en ese escenario, extremadamente complejo, muy visible a veces, y con gran impacto social, otras oculto como una nueva forma de victimización, logrando una mayor presencia internacional con el fin de participar y cooperar en estos delitos en los que se difuminan las fronteras, así como influir en los diferentes foros sobre tecnología y legislación, mejorando también la formación técnica necesaria para atajar ese tipo de delincuencia».*

La **Comisaría General de Policía judicial**[11] está integrada entre otras unidades, por la **Unidad de Investigación Tecnológica**, que asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica. Actuará como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía. De esta Unidad dependerán, entre otras, la **Brigada Central de Investigación Tecnológica**, a la que corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad

[11] Art. 7 de la Orden INT/28/2013, de 18 de enero.

intelectual e industrial y los fraudes en las telecomunicaciones, y la **Brigada Central de Seguridad Informática** la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes.

La **Comisaría General de Policía Científica**[12], está integrada entre otras por la **Unidad Central de Criminalística**, que asume las funciones de estudiar y realizar los informes periciales, de interés policial y judicial, en materia de falsificación documental, grafoscopia, balística forense identificativa y operativa, trazas instrumentales, acústica forense e informática forense, así como la elaboración de los informes periciales, de interés policial y judicial, relacionados con las materias de su competencia.

Una de las secciones de la Unidad Central de Criminalística es la **Informática Forense**. La Sección de Informática Forense se encuentra dividida a su vez en dos grupos: el **Grupo de Análisis de Software**, que se encarga de extraer y analizar la información de soportes digitales, discos duros, disquetes, discos CD o DVD, soportes de memoria *flash,* etc. y el **Grupo de Telefonía Móvil y Electrónica**, que extrae y analiza la información de dispositivos de telefonía móvil y todo tipo de dispositivos electrónicos. Existen además **Grupos Territoriales de Informática Forense** en las Provincias con más incidencia en este tipo de análisis, capaces de dar una primera respuesta más ágil.

1.5.1.1. Actividad de la Sección de Informática Forense

La actividad del laboratorio de Informática Forense[13] está ajustada a un *Manual de normas de Procedimiento* en el que se concretan todas las operaciones de cada proceso, constituyendo un protocolo de actuación que unifica y sistematiza el tratamiento de las evidencias. La normativa internacional que afecta a su actuación entre otras, está contenida en la ISO 17020/17025: *Estándar de calidad en organismos de inspección y de competencia en laboratorios de calibración y ensayo,* y en la ILAC-G19: 2002: *Guía para los laboratorios de ciencia forense*; La sección de Informática forense ha participado asimismo en la elaboración de documentos como la *"Guía de Buenas Prácticas en el Examen Forense de Tecnología Digital"*, así como en la norma ISO 27037: *Guía para la identificación, recogida, adquisición y salvaguardia de la evidencia digital.*

---

[12] Art. 10 de la Orden INT/28/2013, de 18 de enero.

[13] MARTÍN GARCÍA, J. en su artículo *"Pericial informática Forense: Aseguramiento y análisis de evidencias digitales"* en I CONGRESO CIENTÍFICO DE LA ABOGACÍA DEL PRINCIPADO DE ASTURIAS. *"Libro de ponencias",* op. cit., (pp.115 y 116).

En cuanto a la actividad forense, el primer requisito de admisibilidad consiste en que sólo se procesan aquellos elementos que hayan sido intervenidos a través de un procedimiento legal, con una correcta cadena de custodia y la correspondiente autorización judicial para proceder al estudio, por la especial protección de que gozan los datos que normalmente contienen. Se requiere también la clara descripción del objeto del informe pericial, para lo cual se dispone de un *Formulario de solicitud* estandarizado que facilita a las unidades de investigación la aportación de los datos necesarios. Comprobados estos requisitos se realiza un estudio preliminar de todos los objetos recibidos, dando una descripción técnica y detallada de los mismos, fotografiándolos y haciendo alusión a los posibles deterioros que pudieran poseer para dejar constancia de ello en el informe que se emita. Siempre que sea posible se realiza una copia exacta de la información contenida en la evidencia para analizarla, de modo que el original queda inalterado y puede usarse para obtener una nueva copia de trabajo si es necesario y como prueba en el proceso judicial, calculándose una firma digital o *hash* de la evidencia original para garantizar su integridad. El análisis se realiza en un equipo forense totalmente aislado de cualquier tipo de red y con herramientas cuyo impacto sobre el sistema estudiado esté completamente determinado. En el caso de que se utilice una *imagen forense* (copia en un archivo de toda la información contenida en el disco) el análisis debe efectuarse mediante una aplicación forense específica que proporciona de forma lógica esta capa de protección de integridad; Ejemplos de Software forense son programas como Encase, X-Ways, FTK , Sleuthkit, Autopsy, Helix, o Caine. La descripción de todas las tareas de análisis practicadas y sus resultados se detallan en el informe pericial que incluye además, en soporte electrónico, copia de los archivos de interés extraídos de los soportes objeto de análisis, que permiten a la Autoridad Judicial acceder de forma sencilla a las evidencias obtenidas.

1.5.2. Guardia Civil

Al igual que en el Cuerpo Nacional de Policía, en la Guardia Civil se creó a mediados de los años 90 un Grupo especializado en Delitos Telemáticos. En la actualidad su estructura orgánica se regula en la Orden PRE/422/2013, de 15 de marzo, por la que se desarrolla la estructura orgánica de los Servicios Centrales de la Dirección General de la Guardia Civil.

A la **Jefatura de Policía Judicial**[14], al mando de un Oficial General de la Guardia Civil en situación de servicio activo, le corresponde organizar y gestionar la investigación y persecución de los delitos y faltas y desarrollar los servicios de criminalística, identificación,

[14] Art. 10 de la Orden PRE/422/2013, de 15 de marzo.

analítica e investigación técnica, llevando a cabo las funciones de Policía Judicial específica de la Guardia Civil, así como la colaboración en dichas materias y en su propio ámbito corporativo, con otros cuerpos policiales nacionales y extranjeros. De la Jefatura de Policía Judicial dependen, entre otras, la **Unidad Central Operativa (U.C.O.)**, que tiene como misión investigar y perseguir los asuntos relacionados con la delincuencia grave, nacional e internacional y aquella otra cuyas especiales características así lo aconsejen; así como establecer y mantener el enlace, coordinación y colaboración con otros servicios afines, nacionales e internacionales, en el desarrollo de sus investigaciones, haciendo propuestas a la Jefatura de Policía Judicial sobre la gestión de la información de carácter operativo procedente de estos servicios. Dentro de la U.C.O. se creó en 1996 el Grupo de Delitos Informáticos (G.D.I), posteriormente pasó a denominarse Departamento de Delitos de Alta Tecnología (DDAT), siendo su nombre en la actualidad el de **Grupo de Delitos Telemáticos (G.D.T.)**. En cada una de las provincias de España existen **Equipos de Investigación Tecnológica (EDITE)**[15].

1.5.3. La investigación de delitos en Internet

Tanto la Policía como la Guardia Civil emplean múltiples fuentes de información en su labor preventiva, como son la colaboración ciudadana, sus propias investigaciones[16] e, incluso, datos suministrados por colaboradores o confidentes policiales[17], en una fase preliminar o pre-procesal. Una forma habitual de iniciar investigaciones policiales en delitos vinculados a Internet, especialmente los relacionados con la pornografía infantil[18], son los rastreos policiales en Internet para desenmascarar la identidad críptica de las direcciones IP *(Internet Protocols)* que accedan a los *hash* de archivos que contengan pornografía infantil

[15] Información extraída de la página web http://www.guardiacivil.es

[16] STS 1058/2006 de 2 de noviembre, sobre doctrina constitucional relativa al valor probatorio del atestado policial.

[17] STS 654/2013 de 26 junio.

[18] STS 785/2008 de 25 de noviembre: *«La policía conoce y observa en la página Web http// groups.msn.com/fotobaby las 44 fotografías referidas a actos pornográficos de menores y con el fin de identificar el origen en la red de tales fotografías interesa a la autoridad judicial mandamientos para que la Cia. Telefónica facilite la titularidad de la terminal de ordenador, que tenía conexión con el número de teléfono NUM003, al que se asignó la dirección IP (Internet protocol) nº NUM004. Tal prueba es plenamente válida, desde el momento que pudo dar razón de tal diligencia y su autenticidad el policía que la practicó cuando después declaró en juicio».*

en redes P2P[19]. La huella de entrada queda registrada siempre y no es necesaria autorización judicial para obtener las identificaciones de las direcciones IP involucradas en la descarga de archivos pedófilos, dado que *«no es preciso para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma; sin embargo, para lo que sí es necesario acudir a la autorización del juez instructor es para conocer la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data)»*. Así lo reconocen las SSTS 842/2010 de 7 de octubre, 739/2008 de 12 de noviembre y 680/2010 de 14 de julio. En otras ocasiones, se emplea el concepto de *huella informática* como rastro que el sistema conserva, aún después del borrado en la denominada *papelera de reciclaje* y que es capaz de recuperar algún signo de lo inicialmente archivado, para referirse a archivos borrados que son posteriormente recuperados mediante *«sofisticados métodos informáticos»*, como se deduce de la STS 373/2011 de 13 de mayo.

Respecto al carácter de la dirección IP y su obtención por la Policía, la STS 16/2014 de 30 de enero resume la doctrina jurisprudencial, reconociéndola como dato personal[20], y aclarando que las claves identificativas de IP no concretan quién es el usuario, sino únicamente el ordenador que se ha empleado; sólo con autorización judicial podrá obtenerse datos como el número de teléfono y titular de contrato. Esta sentencia razona críticamente, que una vez que se ha admitido la posibilidad de que por la Policía se averigüe la numeración de una IP, no puede presumirse que su obtención lo haya sido por medios irregulares o ilegítimos que vulneren derechos fundamentales, dado que supondría la paradoja de que mientras tratándose de acusados ha de presumirse su inocencia mientras no se pruebe su culpabilidad , parece que a los Tribunales y Fuerzas del Orden, en idéntico marco procesal pretende presumirse una actuación contraria a la Constitución y a las Leyes, en tanto no se pruebe que ha actuado conforme a Derecho. Por ello, aceptar una petición de nulidad de la obtención por la Policía de direcciones IP porque la legitimidad no puede presumirse, no resulta exigencia del vigente sistema de garantías, como recogen las SSTS 249/2008 de 20 de mayo, 960/2008 de 26 de diciembre, 972/2010 de 4 de octubre y

---

[19] ATS 398/2014 de 13 de marzo: *«Hemos indicado, en Sentencia nº 105/2009, de 30 de enero, que el dolo de compartir archivos recibidos que son puestos en la red a disposición de terceros, se puede inducir de una serie de elementos, para lo que se tendrá en cuenta la estructura hallada en el terminal (archivos alojados en el disco o discos duros, u otros dispositivos de almacenamiento), el número de veces que son compartidos (pues este parámetro deja huella o rastro en el sistema informático), la recepción por otros usuarios de tales imágenes o vídeos como procedentes del terminal del autor del delito, y cuantas circunstancias externas sean determinadas para llegar a la convicción de que tal autor es consciente de su actividad de facilitar la difusión de pornografía infantil, entre las que se tomará el grado de conocimiento de la utilización de sistemas informáticos que tenga el mismo».*

[20] SSTS 249/2008 de 20 de mayo, 236/2008 de 9 de mayo, 680/2010 de 14 de julio y 292/2008 de 28 de mayo.

940/2008 de 18 de diciembre, en las que se apuntan casos en los que se cuestionó la forma de obtener números de teléfono por la Policía, estableciendo como valida tal obtención porque no se acredita que hubiese vulneración del secreto de comunicaciones y concluye que *«según criterios de la Sala, no es preciso acreditar la forma de obtención del número de teléfono de un sospechoso cuando no hay indicios de ilegitimidad en el proceso de obtención de la información, pues es exigible a los poderes públicos que justifiquen que la restricción de un derecho fundamental se ha realizado con respeto a las reglas, pero no lo es que demuestren que no lo han hecho[21]».*

En otros casos, pueden obtener información de redes sociales y aportarla a la investigación sin que eso suponga vulneración de Derechos Fundamentales, en este sentido, la SAN (Sala de lo Contencioso-Administrativo, sección 1ª) nº de rec. 577/2011 de 2 de enero de 2013:

> *«Finalmente tampoco cabe apreciar la vulneración de derecho fundamental alguno en cuanto a la aportación por la policía de fotogramas del videoclip en cuestión, por cuanto fueron obtenidos de la red social Facebook, en la que eran accesibles en abierto para cualquier usuario de la misma y con ocasión de la investigación de los hechos denunciados. El hecho de que no se tomara declaración al hoy recurrente en el atestado policial en el que no se adoptó ninguna medida cautelar contra él, no puede considerarse como vulneración del derecho a ser oído, ya que lo relevante al objeto de garantizar su derecho de defensa es que ha sido oído en vía administrativa con carácter previo a la imposición del apercibimiento, por lo que no cabe apreciar ningún tipo de indefensión».*

Respecto a la intervención de soportes electrónicos, la STS 1025/2013 de 26 de diciembre recoge lo siguiente:

> ***«****Valga recordar lo ya dicho en la STS nº 830/2013 de 7 de noviembre : como ha señalado la Circular 1/2013 de la FGE, la apertura de archivos de un disco duro o de unidades externas tampoco afecta al derecho al secreto de las comunicaciones. Se considera más bien el cuerpo de los delitos informáticos. Por ello no es en todo caso imprescindible la autorización judicial, a salvo, como se expuso supra, el acceso a correos electrónicos. Los documentos no integrados en un proceso de comunicación y almacenados en archivos informáticos bien en teléfonos móviles, ordenadores o asimilados, tendrían la consideración de simples documentos y, por tanto, sólo resultarían, en su caso protegidos por el derecho a la intimidad (STS 782/2007 de 3 de Octubre). Por ello los Cuerpos y Fuerzas de Seguridad del Estado pueden, sin autorización judicial, intervenir un soporte magnético o electrónico, como, por ejemplo, la lectura de un disco duro, aun cuando su contenido material pudiera afectar al derecho a la intimidad del art. 18.1*

[21] SSTS 509/2009 de 13 de mayo, 309/2010 de 31 de marzo y 849/2013 de 12 de noviembre.

CE, si se aprecian razones de urgencia y se persigue un interés constitucionalmente legítimo con base en la habilitación legal para dicha actuación reconocida en los arts. 282 LECrim y 11.1 L.O. 2/1986 de 13 de Marzo, de Fuerzas y Cuerpos de Seguridad, y 547 LOPJ. En este sentido, vid. STC 173/2011, de 7 de noviembre , en relación con la investigación de un delito de pornografía infantil».

La forma habitual de proceder en la **investigación de delitos relativos a la pornografía infantil**, normalmente vinculada a medios informáticos o electrónicos, queda reflejada en la SAP de Madrid, sección 17ª, 897/2013 de 1 de julio: tras realizar rastreos en Internet por la Policía Nacional (Unidad de Delincuencia Especializada y Violenta, Grupo de Delitos Tecnológicos, de la Brigada Provincial de Policía Judicial de Valencia) se inicia una investigación en relación a la presunta comisión de un delito de corrupción de menores por tenencia y difusión de material pornográfico infantil, investigando si los concretos titulares de los ordenadores con unas determinadas direcciones IP, estaban descargando y compartiendo un archivo videográfico de contenido pedófilo, a través del programa Emule, archivo perfectamente identificado con un determinado *hash*[22], tras ser examinado por los agentes en el propio programa Emule. A raíz de estas actuaciones preliminares, el Juzgado de Instrucción correspondiente incoa Diligencias Previas librando las oportunas autorizaciones para que las compañías telefónicas facilitaran la identidad del titular, lugar de instalación, de las direcciones IP que estaban siendo utilizadas un día concreto, a una determinada hora en la que se estaba descargando tal archivo. A raíz de la información proporcionada, el Juzgado de Instrucción, decretó mediante auto, la entrada y registro en el domicilio desde donde se realizaron las descargas, especificando en dicho auto que la diligencia se practicaría por funcionarios del Cuerpo Nacional de Policía y en presencia del Secretario Judicial y del Letrado de oficio, a fin de que se pudiese realizar una inspección de los ordenadores ubicados en el domicilio aludido así como para proceder a la intervención de los distintos dispositivos informáticos de almacenamiento en los pudieran hallarse pruebas e indicios que sirvieran para el esclarecimiento de un delito de distribución de pornografía infantil a través de Internet. En acta de la diligencia de entrada y registro levantada bajo la fe pública del Secretario Judicial del Juzgado de Instrucción correspondiente, se hizo constar la notificación del auto de entrada y registro con entrega de copia al titular de la IP, accediendo después al lugar donde realizaba su actividad, procediendo los agentes a examinar los dispositivos informáticos encontrados, con el programa Everest, para conocer el contenido del ordenador, mientras buscaban material electrónico y de almacenamiento, como CDs, discos duros externos, memorias USB etc. En el ordenador analizado se realizó una búsqueda manual de posibles archivos con el

[22] Nombre de identificación originaría, único y permanente del archivo.

contenido investigado localizando en la ruta G:\Incoming (carpeta de archivos compartidos de Emule) tres archivos con contenido normalmente pedófilo. Seguidamente un agente utilizó el programa Perkeo, diseñado para localizar archivos con contenido pedófilo y así, en caso de encontrar archivos de contenido pedófilo, estos se intervendrían, así como en el caso de dispositivos de almacenamiento externo. Por último, los funcionarios encargados del Registro en el acto del Juicio, tendrían que declarar para ratificar lo certificado por el Secretario Judicial.

2. ASPECTOS PROCESALES

2.1. ¿FUENTES O MEDIOS DE PRUEBA?

El artículo 24 de la Constitución de 1978, en su apartado 2, recoge que todas las personas tendrán derecho a utilizar los medios de prueba pertinentes para su defensa mientras que el artículo 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, regula que no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales. Por tanto se podría concluir que se admiten todos los medios de prueba que no lesionen derechos o libertades fundamentales en su obtención, en este sentido la STS 100/2014 de 18 de febrero:

> ***«****Conviene recordar a estos efectos que el artículo 11.1 de la LOPJ dispone que no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales. Indirectamente ha de entenderse, como ha señalado el Tribunal Constitucional (ATC 282/1993) como una referencia a aquellas ocasiones en las que se ha producido una previa conculcación de un derecho fundamental que de manera inmediata no proporciona material probatorio, pero lo obtenido sirve para conducir de forma mediata hasta otra fuente de prueba. El sentido del precepto implica no solo que no es posible valorar las pruebas obtenidas directamente con la vulneración del derecho fundamental, sino también que no pueden ser utilizados legítimamente como medios de investigación, o como datos para iniciar u orientar una investigación penal, aquellos que hayan sido obtenidos violentando los derechos o libertades fundamentales».*

Como señala VEGAS TORRES[23], la extensión del empleo de los ordenadores en numerosas facetas de la vida humana tiene importantes repercusiones en el campo de la prueba procesal. Salvo los casos excepcionales en que se exige por la ley, la prueba de la

[23] VEGAS TORRES, J. *"Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa"*. Cátedra de Investigación Financiera y Forense KPMG-URJC, Universidad Rey Juan Carlos, Madrid 2011, (pp.14 y 15).

existencia y vigencia de normas jurídicas, la prueba procesal tiene normalmente por objeto hechos o máximas de la experiencia. En relación con la prueba de hechos, el empleo de los ordenadores personales y, más en general, de las TIC tiene dos grandes vertientes: la utilización de dichas tecnologías para preconstituir prueba de los actos y negocios jurídicos, o para expedir certificaciones y testimonios del contenido de registros públicos, expedientes administrativos o procesos jurisdiccionales. En este ámbito, en el de los hechos, se sitúan las cuestiones relacionadas con la contratación y la firma electrónicas y la utilización con fines probatorios, principalmente en el proceso civil, de documentos en soporte electrónico (vid. arts. 267 y 268 LEC) así como de los "instrumentos" a que se refiere el art. 384 LEC, que permiten *«archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase»*. Pero el uso de los ordenadores personales y tecnologías relacionadas, para la prueba de hechos, tiene también una segunda vertiente, referida a la prueba de las actividades que un usuario lleva a cabo con un ordenador personal. No se trata en este caso de materiales digitales específicamente creados para la prueba de hechos, sino de los materiales digitales generados por el uso del ordenador, que quedan almacenados en éste (o en un equipo remoto) y permiten conocer la actividad desarrollada por el usuario (escribir un informe, almacenar y retocar unas fotografías, acceder a determinados contenidos de internet, enviar un mensaje de correo electrónico, etc.). Esta última vertiente del uso de los ordenadores personales con fines de prueba, requiere el acceso a los archivos que permiten conocer la actividad de cuya prueba se trata, lo que puede plantear problemas relacionados con derechos fundamentales de la persona cuya actividad se investiga, que surgen, fundamentalmente, cuando se trata de obtener la prueba de actividades del usuario de un equipo informático sin el consentimiento de dicho sujeto, lo que implica que un tercero, sin consentimiento del usuario, accede a los archivos generados por la actividad de éste lo que puede afectar a los derechos fundamentales que protegen la privacidad.

En el ámbito civil y por aplicación supletoria al resto de jurisdicciones, los medios de prueba se regulan en el artículo 299 en la Ley 1/2000, de 7 de enero, Enjuiciamiento Civil, enumerando los siguientes: 1.ºInterrogatorio de las partes. 2.º Documentos públicos. 3.º Documentos privados. 4.º Dictamen de peritos. 5.º Reconocimiento judicial. 6.º Interrogatorio de testigos. Ningún precepto de la LEC se refiere específicamente a la prueba informática, sino que según su forma de aportación podríamos encuadrarla en cualquiera de los supuestos del artículo 299 LEC. Respecto a los medios de prueba, como señala GOMEZ DE LIAÑO[24], el tercer apartado del artículo 299 de la LEC confirma que estamos ante un sistema de *numerus apertus*, que responde a dos finalidades: adaptarse a los avances tecnológicos

[24] GÓMEZ DE LIAÑO GONZÁLEZ, F. *"El proceso civil"*. Editorial Forum, Oviedo 2005, (p.180).

y admitir todo aquello que proporcione un conocimiento de las cosas, eliminando formalidades que no responden a la concepción actual del Derecho procesal. Por el contrario, otros autores, como ABEL LLUCH[25] optan por hacer una distinción conceptual entre medios de prueba y fuentes de prueba, considerando que aún cuando este tercer apartado del artículo 299 de la LEC alude a *«cualquier otro medio no expresamente previsto en los apartados anteriores»*, se refiere a cualquier otra fuente de prueba, puesto que los medios son limitados y las fuentes ilimitadas, en consecuencia al tratarse de nuevas fuentes de prueba podrán aportarse al proceso a través de la regulación contenida en los artículos 382 a 384 de la LEC. También entiende este autor, que hubiera sido preferible acoger un concepto amplio de documento, que fuera comprensivo de los recogidos en soportes audiovisuales o electrónicos, y admitir que las TIC accedieran al proceso a través de la aportación de documentos y cualesquiera otros medios de prueba, teniendo en cuenta sus particularidades en orden a su aportación a las actuaciones y la garantías para preservar su autenticidad.

Tampoco en la jurisdicción penal encuentran su sitio; como manifiesta PORTAL MANRUBIA[26], pocas disposiciones regulan la utilización de las TIC en la Ley de Enjuiciamiento Criminal. Los artículos 306, 325, 448, 731 bis y 743 de la LECRIM permiten que el Ministerio Fiscal, el imputado, testigo o perito actúen en fase de instrucción o durante el desarrollo del juicio oral por medio de un sistema que permita una comunicación bidireccional y simultánea siendo conservadas dichas actuaciones en un documento electrónico. En la LOPJ, en su artículo 230, se reconoce a las partes la posibilidad de emplear cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, cuando sean compatibles con los que dispongan los Juzgados y Tribunales y se respeten las garantías y requisitos previstos en el procedimiento de que se trate. Las disposiciones relativas a la práctica de la prueba en el proceso penal se recogen en los artículos 688 a 731 de la LECRIM. Como señala MEDRANO I MOLINA[27], respecto a la prueba documental –que es a través de la cual se introducen los soportes informáticos y audiovisuales en el proceso penal, dada la amplitud del concepto de documento del art. 26 del Código Penal[28]– su

---

[25] ABEL LLUCH, X. en su artículo *"Nuevas Tecnologías y acceso al proceso"*, en ABEL LLUCH, X. PICÓ I JUNOY, J. RICHARD GONZALEZ, M.(coords.) *"La prueba judicial, desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa"*, op. cit., *(*pp. 352 a 366).

[26] PORTAL MANRUBIA, J. *"La regulación de la prueba electrónica en el proceso penal"*. Revista Aranzadi de Derecho y Proceso Penal, mayo - agosto 2013, (pp. 19 a 41).

[27] MEDRANO I MOLINA,J.M. *"Práctica de la prueba por soportes informáticos y audiovisuales en el proceso penal",* Universitat de València, (pp. 7 a 10).

[28] Artículo 26 CP: *«A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica».*

regulación se contiene específicamente en el artículo 726[29], además, en sede de disposiciones comunes, encontramos el artículo 730 que permite la lectura en el Juicio oral de las diligencias practicadas en el sumario que no puedan ser reproducidas en el mismo, disposición que tendrá gran relevancia en el caso de la prueba por soportes informáticos y audiovisuales, asimismo, señala que la prueba por soportes informáticos, por su encuadre en la prueba documental penal[30], puede acceder al proceso, y más en concreto, al acto del juicio oral, a través de tres vías: a) Lectura b) Examen por el propio Tribunal c) Indirectamente, a través de una pericia documental.

2.2. INCORPORACIÓN AL PROCESO

La forma más habitual de incorporar las pruebas obtenidas de dispositivos informáticos y electrónicos al proceso es la documental, bien como documento público o como documento privado, normalmente acompañada de la prueba pericial oportuna.

2.2.1. Prueba documental

2.2.1.2. Documento privado

Si una parte aporta como prueba documental un e-mail impreso, un historial de conversaciones de Whatsapp o una captura de pantalla de una página web o de una red social, su valor probatorio dependerá, entre otras cuestiones, de la actitud de la parte a quien perjudiquen. Según el artículo 326 de la LEC, si no se impugna su autenticidad, hará prueba plena del contenido, fecha y personas que hayan intervenido, como recoge el artículo 319 de la LEC para los documentos públicos. Si, por el contrario, se impugna, quien lo haya presentado podrá proponer prueba pericial para acreditar su autenticidad y en todo caso, según el artículo 326 de la LEC en su apartado segundo, si no se pudiese deducir su autenticidad o no se propusiese prueba alguna el Tribunal lo valorará según las reglas de la sana crítica. En el apartado 3 del citado artículo se regula que en el caso de que la parte a

---

[29] Art. 726 LECRIM: *«El Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad».*

[30] En este sentido, la SAP de Madrid, secc. 17ª, 897/2013 de 1 julio, rec. 52/2011: *«Más relevante consideramos el testimonio del funcionario de Policía Nacional nº NUM006 que intervino en el acto de juicio oral en calidad de testigo y de perito y la documentación -prueba documental- en su día remitida por éste al Juzgado de Instrucción e incorporada a las actuaciones. Así, este funcionario policial aportó a las actuaciones un informe adjuntando numerosas documentación -prueba documental-, en soporte papel -acompañando numerosas fotografías de la imagen de la pantalla del ordenador, lo que comúnmente se llama "pantallazos"- y en soporte digital -CD incorporado a las actuaciones con copia del informe y de los archivos de video examinados estudiado- y que ahora, su posesión y difusión, es objeto de enjuiciamiento».*

quien interese la eficacia de un documento electrónico[31] lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, (en adelante LFE), que establece que el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio y tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable. Si se impugnare la autenticidad de la firma electrónica reconocida[32] con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada[33] basada en un certificado reconocido[34], que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica. La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que se originen con motivo de la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

Una forma de aportar el contenido de mensajes SMS o conversaciones de Whatsapp en un proceso civil, sería proponer como prueba documental la transcripción del texto y solicitar como prueba anticipada el cotejo por el Secretario Judicial, con la exhibición del teléfono móvil para su comprobación, siendo conveniente presentar contrato de línea

---

[31] Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado (art. 3 Ley de Firma Electrónica). Será soporte, entre otros, de documentos privados.

[32] Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

[33] La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

[34] Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

telefónica de quien lo aporta, para verificar que es el titular de la línea y en su caso, solicitar que se libre oficio a la compañía telefónica de la otra parte para comprobar que el número de teléfono que aparece se corresponde. En cambio, en un proceso penal de faltas, se podría llevar directamente al acto del juicio para su comprobación. En este sentido, SAP de Granada, Secc. 2ª, 560/2007 de 19 de octubre:

> ***«****Por otro lado, si realmente se vertieron aquellos insultos mediante mensaje telefónico, ni la declaración en juicio de la denunciante lo ha podido corroborar ya que no consta en el acta que dijera nada sobre ello, y en la hipótesis contraria esa sola declaración habría sido insuficiente para demostrar con plena certeza ese hecho, sabido como es, que los mensajes recibidos vía SMS quedan grabados en el teléfono receptor, y nada más fácil habría sido para la denunciante que aportar al acto del juicio oral como prueba documental el propio mensaje supuestamente insultante con la simple exhibición del aparato y la comprobación del contenido del mensaje».*

Hay que señalar que a veces el borrado de todos los registros de mensajes de Whatsapp con una persona concreta puede indicar que los mensajes obedecían a una actividad ilícita, así, en la SAP de Málaga (sección 7ª, Melilla) 19/2013 de 21 de marzo, el Tribunal entiende que *«si los mensajes que se intercambiaron no obedecían a ninguna actividad ilícita no tenía por qué haberlos borrado, como tampoco borró los mensajes que cruzó con otras personas».*

Respecto al valor probatorio de las conversaciones a través de Whatsapp, la SAP de Valladolid, secc. 2ª, 77/2014 de 10 de marzo recoge lo siguiente:

> ***«****Alega el recurso de apelación que una conversación de Whatsapp es totalmente modificable, y que por ello el documento notarial unido en el acto del juicio no puede constituir prueba alguna de que realmente se hayan producido las conversaciones que se dicen en el mismo. Aporta para ello prueba en esta segunda instancia, pero tal prueba no avala el que tales conversaciones por dicho sistema se puedan modificar. Del contenido de la prueba se acredita que se pueden borrar los mensajes, y que se puede copiar y pegar texto en los mensajes que se envían a otro. Se puede reenviar el contenido a otra persona, pero no se ha aportado prueba alguna que acredite como pretende el apelante que se pueda editar para su modificación un mensaje recibido. (…) Choca pues con principios lógicos y racionales el que el denunciante hubiese modificado el contenido de los mensajes enviados por el denunciado a través del sistema citado. (…) La problemática de la fecha, no incide ni contradice la realidad de los hechos cometidos, recogidos en las conversaciones a través del sistema Whatsapp. No existe error en la valoración de la prueba, en cuanto la documental obrante en las actuaciones, es bastante para la declaración de hechos probados que contiene la sentencia apelada. No existe infracción de doctrina jurisprudencial. La prueba documental es válida».*

Es frecuente en la práctica de los Juzgados y Tribunales aceptar como válidas, previa acreditación de su veracidad, las comunicaciones realizadas a través de SMS o de correos electrónicos, así la SAP de Cáceres, sección 2ª, 444/2013 de 30 de septiembre, admite como válida la comunicación realizada por una progenitora denunciada en una falta de incumpliendo del régimen de custodia, absolviéndola al constar que la existencia de correos electrónicos enviados al otro progenitor demostraba que éste estaba al tanto del cambio de domicilio del hijo común. En el caso de la STS 73/2012 de 20 de febrero, se estimó que el principio de prueba del que debe partirse como momento de fijación del *dies a quo* en una acción de impugnación de la filiación matrimonial en el presente caso, había sido la manifestación de la propia recurrente, mediante el envío de diversos SMS en los que comunicó a su ex marido la no paternidad y le recomendó que efectuara una prueba de ADN, con lo que daba a entender claramente que no era el padre, entendiendo que es a partir de este momento que empieza a correr el plazo de caducidad de la acción de impugnación.

2.2.1.2. Documento público

Su presentación se realizará mediante la intervención de un Notario, ya sea un acta de protocolización[35] de un documento que se le entregue, por ejemplo un correo electrónico impreso en papel, o un acta de presencia[36], como podría ser el caso de una personación del

[35] Según el artículo 211 del Decreto 2 de junio de 1944, por el que se aprueba con carácter definitivo el Reglamento de la organización y régimen del Notariado, tendrán las características generales de las de presencia, pero el texto hará relación al hecho de haber sido examinado por el Notario el documento que deba ser protocolado, a la declaración de la voluntad del requirente para la protocolización o cumplimiento de la providencia que la ordene, al de quedar unido el expediente al protocolo, expresando el número de folios que contenga y los reintegros que lleve unidos.

[36] Según el art. 199 del Reglamento del Notariado, acreditan la realidad o verdad del hecho que motiva su autorización. El notario redactará el concepto general en uno o varios actos, según lo que presencie o perciba por sus propios sentidos, en los detalles que interesen al requirente, si bien no podrá extenderse a hechos cuya constancia requieran conocimientos periciales.

Notario en un lugar virtual, como una página web[37], o una bandeja de entrada y posterior lectura de un correo electrónico. Sus impresiones las recogerá el acta, que en este caso tiene mayor efecto probatorio al extenderse la fe pública notarial también a los contenidos, a las que se suele añadir "pantallazos" del teléfono móvil o del ordenador examinado. La eficacia probatoria es la recogida en el artículo 319 de la LEC, por tanto harán prueba plena del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan en ella.

2.2.2. Prueba pericial

Como afirma PASAMAR[38], refiriéndose a la prueba y su contexto digital, un archivo de texto guardado en un ordenador ha de analizarse en el contexto de ese ordenador, porque en el caso contrario se perdería información clave para mantener la coherencia del análisis, todo ello, porque en el medio digital es muy difícil diferenciar el archivo original de sus copias, debiendo buscarse siempre la coherencia de la prueba en la conservación de la mayor cantidad de información posible.

Problemas como la volatilidad y alterabilidad afectan especialmente a las pruebas informáticas, por lo que es muy recomendable que el análisis lo realice un experto en evidencias digitales con conocimientos adecuados de informática forense, definida por

---

[37] SAP de Valencia (Sección 9ª) núm. 253/2011 de 15 de junio: *«Se ha aportado por la demandante acta notarial de 30 de julio de 2009 - folio 71 y los siguientes - de la que resultan los contenidos de los textos objeto de debate en el presente procedimiento correspondientes a cada una de las dos páginas web controvertidas.(…) De los contenidos de los "pantallazos" de ambas páginas en conflicto incorporados a los folios 94 a 100 de las actuaciones se observa - con referencia a la fecha en que fueron realizados - la existencia de textos comparativamente idénticos en su redacción y disposición, del mismo modo que en el acta notarial de 30 de julio de 2009. Consideramos que la actora ha cumplido con la carga de la prueba al aportar a las actuaciones las imágenes de pantalla de las respectivas páginas web obtenidas a presencia notarial en fecha 30 de julio de 2009, tras el proceso que se describe en la diligencia levantada al efecto, mediante el procedimiento de entrada en la red y visualización del contenido de las páginas web a través del ordenador, quedando constancia de dicho contenido con referencia al momento temporal en que se hacen tales comprobaciones por fedatario público y se procede, al mismo tiempo, a su impresión para plasmar sobre el papel el contenido digital de la información objeto de comprobación, como hiciera, a su vez, la parte demandada, para probar, en febrero de 2010, que había retirado los contenidos controvertidos de su página. Cierto es que la sentencia se refiere especialmente a los documentos 17 a 23 consistentes en simples pantallazos impresos, pero lo que se ha venido a discutir sobre ellos en la primera instancia no es que no se correspondan con la realidad de lo existente en el momento de su impresión sino que los contenidos de los textos que aparecen en una y otra página (párrafos literales en muchos casos, o con pequeñas precisiones de referencia a cada de una de las respectivas entidades litigantes) sean susceptibles o no de protección desde la perspectiva de la Ley de Propiedad Intelectual, que es una cuestión distinta».*

[38] PASAMAR,A., ORMAZÁBAL SÁNCHEZ,G., BELLIDO ASPAS,M. *"Empresa y prueba informática"*. Bosch, Colección de formación continua Facultad de Derecho de Essade, Barcelona 2006, (p. 24).

MARTÍN GARCÍA[39] como *«La disciplina científica de adquirir, preservar, obtener y presentar datos relacionados con un hecho delictivo que han sido procesados electrónicamente y guardados en soportes informáticos, electrónicos o terminales de telefonía móvil, teniendo su fundamento en las leyes de la física, de la electricidad y el magnetismo, obteniendo de este modo lo que denominamos "Evidencia Digital" y poniendo esta a disposición de los jueces a través del informe pericial. Todo ello gracias a fenómenos electromagnéticos que permiten que la información se pueda almacenar, leer e incluso recuperar cuando se creía eliminada. Esta labor tiene especial trascendencia en los denominados "delitos tecnológicos" pero con el impacto actual de las nuevas tecnologías en todos los aspectos de la vida, especialmente el social, la tipología delictiva a que puede aplicarse es la práctica totalidad».*

La manera de proceder[40], en una pericial de este tipo, sería asegurar el escenario en el que se ha producido el incidente informático, intentando extraer la mayor información posible. Para asegurar el escenario, el perito se valdrá de funciones matemáticas llamadas *funciones de hash,* éstas se aplican sobre la información que se adquiere, la cuál se copia, y la identifican como única, de manera, que si se volviesen a aplicar sobre la información original o sobre cualquiera de sus copias, siempre devolverían el mismo identificador, en caso contrario, significaría que la información ha sido alterada de forma deliberada o accidental, motivo por el que el perito al acceder al escenario debe realizar copias, calcular los *hashes* y custodiar la información obtenida adecuadamente, por ejemplo depositando tanto la información como los *hashes* ante Notario. Es de gran importancia que quede reflejado cómo se adquirió la información, especificando si fue ante Notario, si había testigos, o si estaba presente la persona investigada, y si posteriormente se realizó un acta y si los testigos recibieron copia de los *hashes*. Asimismo, si se adjuntaron fotografías o vídeo, y por último si el proceso quedó registrado en documento público, aumentando su valor probatorio. Los resultados de un análisis bien realizado pueden revelar multitud de datos, algunos aparentemente ocultos, e incluso sería posible recuperar datos borrados tras haber sido formateado el disco, o encontrar fragmentos de mensajería instantánea, correo o históricos de navegación, así como alteraciones deliberadas de fechas y contenidos de

---

[39] MARTÍN GARCÍA, J. en su artículo *"Pericial forense: aseguramiento y análisis de las evidencias digitales"* en I CONGRESO CIENTÍFICO DE LA ABOGACÍA DEL PRINCIPADO DE ASTURIAS. *"Libro de ponencias"*, op. cit., (pp.116 y 117).

[40] STS 342/2013 de 17 de abril: *«La transcripción en el acta del desarrollo de la prueba pericial es de especial interés. Concurren los peritos de ambas partes. Por el agente de policía núm. NUM063 se describe el mecanismo formal de solicitud y cesión de los datos, primero a Microsoft, luego a Telefonica y a ONO-central. Se recuerda la cobertura de ambas peticiones con los correspondientes mandamientos judiciales. Describe el perito que, una vez en su poder el CD ofrecido por la empresa que gestiona el programa de mensajería, se abre con la contraseña y estudian las IPs de conexión, junto con su fecha y hora, datos muy importantes en las IPs dinámicas y que ese CD viene protegido por contraseña para evitar que, dado que se envían por correo, cualquier persona lo pudiera consultar».*

archivos. Desde luego, las posibilidades son infinitas. En el análisis forense, dos aspectos que deben tenerse siempre en cuenta por su gran importancia y posterior transcendencia son por un lado, la cadena de custodia de la información, garantía para posteriores profesionales que deban analizar la información en el futuro con los programas correspondientes, y por otro lado, evitar la vulneración de los derechos fundamentales durante la obtención y posterior análisis de la información, poniendo especial cuidado en no revelar informaciones personales o privadas que impliquen una intromisión en el derecho a la intimidad o al secreto de comunicaciones, siempre desde el principio de proporcionalidad y las normas del artículo 335 y siguientes de la LEC.

Pueden establecerse varios análisis periciales distintos, uno de ellos sería el que tiene por objeto analizar la fuente de la prueba, y tratar de establecer que la prueba obtenida no ha sido manipulada y que no se ha roto la cadena de custodia, siendo su finalidad garantizar su integridad, entendida como ausencia de manipulación o alteración de la autenticidad de la fuente de la prueba. Otro tipo de pericia es análisis de contenidos, por ejemplo establecer si un programa informático es auténtico o es una copia no autorizada que vulnera derechos de propiedad intelectual; Y en otros casos, su misión será recuperar archivos ocultos[41], encriptados[42] o eliminados del dispositivo informático. Respecto al borrado de archivos, el AAP de Barcelona, secc. 15ª, 46/2006 de 2 de febrero recoge lo siguiente:

> ***«****En nuestro caso, el perito informático de las demandantes no interfirió un proceso de comunicación ajeno. Puede discutirse, y así se hará, la posibilidad del empresario de acceder al correo electrónico de su empleado, pero ni siquiera en ese caso podría obviarse algo sustancial del caso que nos ocupa, como es que el Sr. Luis Miguel, en un período de siete horas formateó el disco duro, modificó el reloj, modificó el nombre de usuario y reinicializó el sistema operativo del ordenador de la empresa. Esta operación de borrado, que efectivamente fue anunciada por el requerido tras negarse a permitir el acceso a los contenidos del ordenador que utilizaba, supuso deshacer el armazón de dicha información y convertirla en una amalgama de datos no susceptible de clasificación, en la que los datos del correo electrónico se mezclaba de forma indiscriminada con archivos word, excel, imágenes u otros formatos. La búsqueda ciega que el perito llevó a cabo, según opera la herramienta Encase o similares y ratificó el Sr. Bevilacqua, no supone por tanto la lectura de toda la información para detectar lo relevante para la empresa, sino la utilización de palabras clave que sólo permiten rescatar lo que interesa, si es que no hubiera sido borrado en la reinstalación. El borrado usual (pues existen*

[41] Archivos que tienen una contraseña que impide su acceso.

[42] Archivos que han sido codificados, resultando la información que contienen ilegible mientras no sean descodificados.

otros de bajo nivel que sí eliminan la información), no hace desaparecer los datos, sino que elimina las entradas de los mismos y hace imposible acceder a ellos: al romperse el código de entrada en sistema binario, los datos permanecen, pero confundidos e indistinguibles en una enorme cantidad de ceros y unos, de modo que el programa empleado pretende detectar los patrones binarios de ciertas palabras, y una vez detectados, reinterpretar por encima y por debajo hasta reconstruir un texto. Las apelantes utilizan la imagen de un archivador volcado sin orden ni concierto en el suelo, del que se rescata tan sólo una hoja concreta. Pero más gráfica es la idea de un aparato de destrucción de documentos que almacena los restos, del que se rescatan ciertos fragmentos de papel para, mediante su interpretación, reconstruir uno de aquellos documentos. Pretender que la información así obtenida, es decir, los mensajes de correo electrónico rescatados de un ordenador formateado y entregado voluntariamente por su usuario, constituyen una comunicación protegible por la doctrina constitucional expuesta, es exacerbar esa protección: la comunicación no era localizable como tal ex ante y no es que hubiera finalizado bastantes meses atrás, sino que fue deliberadamente destruida por el comunicante, por lo que estuvo muy lejos de cualquier interferencia en un proceso comunicativo ajeno. Los textos reconstruidos podrían ser muestra de una violación a la intimidad de los demandados, pero no una afrenta al secreto de las comunicaciones».

2.2.3. Otras formas de incorporar las NN.TT. al proceso

Dentro de las consideradas pruebas personales, una forma de incorporar las pruebas vinculadas a las NTC es interrogar a las partes o a los testigos acerca del contenido y/o autoría, por ejemplo, de un correo electrónico, comentario realizado en redes sociales como Facebook o Twitter, o el texto de un SMS o Whatsapp, siempre que estos no pudieran aportarse, posibilidad nada descabellada dada la volatilidad de este tipo de pruebas. La eficacia de estas pruebas es diferente según sea interrogatorio de parte, recogido en el artículo 316 de la LEC o testifical, en el artículo 376 de la LEC. Como propone ABEL LLUCH[43], otra opción para incorporar al proceso las nuevas tecnologías sería la cibernavegación o reconocimiento judicial en Internet, que se regula en los artículos 353 y siguientes de la LEC, realizando el examen judicial de un lugar virtual, que desde luego ayudaría a formar una mayor convicción en el juez. Respecto a la prueba testifical como método probatorio de lo manifestado en conversaciones de Whatsapp o Facebook, la SAP Las Palmas, Secc. 2ª, 180/2011 de 15 julio:

«Considera la recurrente que se ha vulnerado el principio de presunción de inocencia al no haberse acreditado la titularidad de la cuenta, del perfil y del número de teléfono asociado al

[43] ABEL LLUCH, X. en su artículo *"Nuevas Tecnologías y acceso al proceso"*, en ABEL LLUCH, X. PICÓ I JUNOY, J. RICHARD GONZALEZ, M.(coords.) *"La prueba judicial, desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa"*, op. cit., pp. 363 a 366.

WhatsApp desde los que se remitieron los mensajes presuntamente denunciados, negando en todo momento la denunciada la autoría de los mismos, basándose la condena en la declaración del testigo, ex novio de la denunciante, quien sostiene haber mantenido la conversación mediante WhatsApp con la misma y otra testigo que al parecer vio en Facebook los comentarios injuriosos que provenían del perfil supuestamente creado por Da Carolina pero sin que dicho particular haya quedado, a juicio de la parte, totalmente acreditado . (…)Teniendo en cuenta todas estas consideraciones ha de concluirse que la sentencia apelada no incurre en error alguno pues valora las manifestaciones de las partes dando más credibilidad a una de las versiones, concretamente a la ofrecida por la denunciante, que se corrobora con las manifestaciones de los testigos. En primer lugar, el ex novio de la denunciante, quien manifestó haber mantenido una conversación mediante el sistema " WhatsApp ", con la denunciada, y en segundo lugar la testigo, conocida de ambos, quien afirmó haber visto en Facebook los comentarios efectuados por la denunciada. Sostiene ahora la defensa que no se practicó prueba alguna para acreditar que el teléfono asociado fuera el de la denunciada o que hubiera ésta creado su perfil de Facebook, sin embargo, tal y como se declara probado en la sentencia de instancia, se trata de mensajes que se producen después de decir la denunciada a la denunciante que "Nachito iba a saber unas cositas", tratándose de una amplia conversación mediante mensajes, en la que al testigo no le cabe duda alguna de que conversaba con Iraya, ofreciendo datos personales que identifican a la denunciada, y declarando en el mismo sentido la testigo Natasha. En cualquier caso se trata de prueba, de carácter personal, que ha sido correctamente analizada, y modificar dicha valoración en esta alzada supondría una nueva valoración de pruebas de carácter personal practicadas en el acto del juicio, sin haber celebrado nueva vista, ni haber podido, por tanto, examinar directa y personalmente a la denunciada y los testigos, con lo que procede la desestimación del recurso interpuesto al estimar la valoración de la prueba practicada, ajustada a derecho».

Otra forma de aportar pruebas vinculadas a las nuevas tecnologías al proceso es el atestado policial[44] resultante de investigaciones en Internet. La doctrina constitucional acerca de su valor probatorio lo resume la STS 1058/2006 de 2 de noviembre:

a) Solo puede concederse al atestado valor de autentico elemento probatorio si es reiterado y ratificado en el juicio oral, normalmente mediante la declaración testifical de

[44] SAP de Madrid, secc. 17ª, 897/2013 de 1 Jul. 2013: *«Más relevante consideramos el testimonio del funcionario de Policía Nacional nº NUM006 que intervino en el acto de juicio oral en calidad de testigo y de perito y la documentación -prueba documental- en su día remitida por éste al Juzgado de Instrucción e incorporada a las actuaciones. Así este funcionario policial aportó a las actuaciones un informe adjuntando numerosas documentación -prueba documental-, en soporte papel -acompañando numerosas fotografías de la imagen de la pantalla del ordenador, lo que comúnmente se llama "pantallazos"- y en soporte digital -CD incorporado a las actuaciones con copia del informe y de los archivos de video examinados estudiado- y que ahora, su posesión y difusión, es objeto de enjuiciamiento».*

los agentes de Policía firmantes del mismo[45]. Ello es así porque únicamente pueden considerarse autenticas pruebas las practicadas en el acto del juicio oral, con posibilidad de debate contradictorio y en presencia del juez para conseguir así, en su caso, la convicción de éste sobre los hechos enjuiciados, mediante el contacto directo con los elementos utilizados. El atestado policial, así como los datos de investigación policiales que constan en el mismo, tienen en principio, únicamente, valor de denuncia, lo que deriva del art. 297 LECRIM. La instrucción previa, se llame diligencias previas o de cualquier otro modo, tiene una naturaleza análoga, si no idéntica a la del sumario, y, como éste, su finalidad consiste en la averiguación del delito y la identificación del delincuente, siendo su función procesal la preparación del juicio oral (art. 299 LECRIM). Ahora bien, lo dicho no significa que las diligencias sumariales (en sentido amplio) e incluso las policiales, carezcan de eficacia probatoria. No cabe negarles tal para desvirtuar la presunción de inocencia si fueron obtenidas con las garantías que la Ley y la Constitución exigen y son reproducidas en el acto de la vista con posibilidad de contradicción por el acusado. En consecuencia, vulnera el derecho a la presunción de inocencia la sentencia condenatoria que se dicte sobre la única base del atestado policial no ratificado (STC 303/93).

b) No obstante lo anterior, el atestado tiene virtualidad probatoria propia cuando contiene datos objetivos y verificables, pues hay partes del atestado, como pueden ser planos, croquis, huellas, fotografías que, sin estar dentro del perímetro de las pruebas preconstituidas o anticipadas, pueden ser utilizadas como elementos de juicio coadyuvantes, siempre que sean introducidos en el juicio oral como prueba documental a fin de posibilitar su efectiva contradicción por las partes[46], por cuanto ninguna de las enumeradas son practicables directamente en el juicio oral por ser imposible su reproducción en idénticas circunstancias. Por lo mismo, las pericias técnicas que se adjuntan al atestado no pierden por ello su propio carácter y constituyen pruebas preconstituidas que despliegan toda su validez probatoria si son incorporadas debidamente al proceso.

c) Por último, en cuanto a su carácter de prueba documental, cabe precisar que el atestado, con independencia de su consideración material de documento, no tiene, como regla general, el carácter de prueba documental, pues incluso en los supuestos en los que los agentes policiales que intervinieron en el atestado presten declaración en

[45] SSTC 100/85, 101/85, 173/85, 49/86, 145/87, 5/89, 182/89, 24/91, 138/92, 301/93, 51/95 y 157/95

[46] SSTC 132/92 y 157/95.

el juicio oral, las declaraciones tienen la consideración de prueba testifical[47]. Solo en los casos antes citados, como planos, croquis, fotografías, etc., el atestado policial puede tener la consideración de prueba documental, siempre y cuando, se incorpore al proceso respetando en la medida de lo posible los principios de inmediatez oralidad y contradicción (STC 175/97 de 14 de octubre).

Por último, podría considerarse la práctica de prueba anticipada y la petición de medidas cautelares sobre dispositivos en equipos informáticos; en este sentido, el Auto de 5 Mar. 2009, proc. 114/2009 del Juzgado de lo Mercantil N°5 de Barcelona y el Auto del Juzgado de lo Mercantil de Bilbao (Provincia de Vizcaya) rec. 277/2005 de 30 de mayo de 2005, en dos casos de posible vulneración de derechos de propiedad intelectual en los que se solicitaron las medidas cautelares consistente en :1º).- Constitución de la comisión judicial, con auxilio de la fuerza pública, y presencia del Secretario Judicial, y peritos informáticos en la sede de la entidad presuntamente infractora de los derechos de propiedad intelectual, para el examen de ordenadores, discos duros, y otros soportes informáticos, con elaboración de informes pericial acerca de su contenido. 2°).- Depósito o consignación de los ingresos de la actividad ilícita, según informe pericial, 3°).- Orden de suspensión de la actividad ilícita y secuestro del material empleado.

3. NUEVAS TECNOLOGÍAS Y VULNERACIÓN DE DERECHOS FUNDAMENTALES DEL ARTÍCULO 18 DE LA CONSTITUCIÓN ESPAÑOLA

3.1. INTRODUCCIÓN

La obtención de pruebas vinculadas a las nuevas tecnologías es especialmente sensible a la vulneración de los derechos fundamentales contenidos en el artículo 18 de la Constitución Española, como son, el derecho al honor, a la intimidad personal y familiar y a la propia imagen, la inviolabilidad de domicilio y el secreto de comunicaciones.

3.2. SECRETO DE LAS COMUNICACIONES (ART. 18.3 CE)

El apartado 3 del artículo 18 CE garantiza el secreto de las comunicaciones y, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial, este derecho está recogido asimismo en la Declaración Universal de los Derechos Humanos en su artículo 12, en el Pacto Internacional de Derechos Civiles y Políticos, en el artículo 17 y en el

[47] STC 217/89.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales en su artículo 8.

3.2.1. Regulación legal

A nivel legislativo este derecho se encuentra afectado, entre otras normas, por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que desarrolla la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio. Esta Ley obliga a las operadoras a conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados[48] siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales, como especifica en su artículo 1.1. El periodo de conservación de los datos, como señala su artículo 5, cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

Otras normas que afectaba este derecho y al resto de los protegidos en el artículo 18 de la Constitución, son la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba su Reglamento, la Ley 32/2003, de 3 de noviembre, General de

[48] Art. 6.2 de la Ley 25/2007. Tendrán la consideración de agentes facultados:
a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.
c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Telecomunicaciones, y el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

3.2.2. Requisitos jurisprudenciales para su restricción

El secreto de las comunicaciones no tiene carácter absoluto, como señala la STS 849/2013 de 12 de noviembre, sino que puede estar sujeto a limitaciones y restricciones, que deberán estar previstas por Ley en función de intereses que puedan ser considerados prevalentes según los criterios propios de un Estado democrático de Derecho, como son la prevención del delito, que constituye un interés constitucionalmente legítimo y que incluye la investigación y el castigo de los hechos delictivos cometidos, orientándose su punición por fines de prevención general y especial[49]. Por tanto, para que tales restricciones puedan hacerse efectivas, es preciso que, partiendo de la necesaria habilitación legal, existan datos que en cada caso concreto pongan de que la medida restrictiva del derecho es proporcional al fin pretendido, que este fin es legítimo y que es necesaria en función de las circunstancias de la investigación y del hecho investigado, lo que implica una valoración sobre la gravedad del delito, sobre los indicios de su existencia y de la intervención del sospechoso, y sobre la necesidad de la medida. La decisión sobre la restricción de este derecho se deja en manos exclusivamente del poder judicial, concretamente, en el Juez de instrucción, a quien corresponde la ponderación de los intereses en juego, mediante un juicio acerca de la proporcionalidad y necesidad de la medida, el cual deberá expresarse en una resolución judicial motivada, adoptada en el ámbito de un proceso penal. Bien entendido que las exigencias de motivación (artículos 24.1 y 120.3 CE), reforzada cuando se trata de restricción de derechos fundamentales, imponen que no sea suficiente la intervención de un Juez, sino que es exigible que tal intervención esté razonada y justificada de forma expresa y suficiente. En el momento de adoptar su decisión, el Juez ha de atender, necesariamente a varios aspectos:

a) **La proporcionalidad**, en el sentido de que ha de tratarse de la investigación de un delito grave. Para valorar la gravedad no solo es preciso atender a la previsión legal de una pena privativa de libertad grave, sino además debe valorarse la trascendencia social del delito que se trata de investigar.

b) **La especialidad**, en tanto que la intervención debe estar relacionada con la investigación de un delito concreto, sin que sean lícitas las observaciones encaminadas

[49] STS 722/2012 de 2 de octubre.

a una prospección sobre la conducta de una persona en general. En este sentido, los hallazgos casuales son válidos, pero la continuidad en la investigación de un hecho delictivo nuevo requiere de una renovada autorización judicial. En este aspecto debe delimitarse objetivamente la medida mediante la precisión del hecho que se está investigando, y subjetivamente mediante la suficiente identificación del sospechoso, vinculando con él las líneas telefónicas que se pretende intervenir. Para ello es preciso que el Juez cuente con indicios suficientes de la comisión del delito y de la participación del investigado.

c) **La necesidad, excepcionalidad e idoneidad de la medida**, ya que, partiendo de la existencia de indicios de delito y de la intervención del sospechoso, suficientemente consistentes, solo debe acordarse cuando, desde una perspectiva razonable, no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado y, potencialmente, también útiles para la investigación.

En cuanto al alcance de la protección formal este derecho y su ámbito de extensión, la STS 83/2014 de 13 de febrero diferencia en función del formato, convencional o tecnológico, que haya servido de vehículo para la comunicación ya agotada, y así, será el derecho a la intimidad (art.18.1 CE) o el derecho a la protección de datos (art.18.4 CE) el que tome el relevo. La jurisprudencia constitucional y del Tribunal Supremo no ha sido lo suficientemente uniforme a la hora de fijar el alcance y límites de la protección formal dispensada por el derecho al secreto de las comunicaciones, así, la STC 114/1984, 29 de noviembre prolongó la protección formal del derecho a la inviolabilidad de las comunicaciones más allá de la interrupción del proceso comunicativo: *«el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje -con conocimiento o no del mismo- o captación de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)»*. En cambio, la STC 70/2002, 3 de abril, asoció los términos de la protección constitucional del derecho a la inviolabilidad de las comunicaciones, al momento en el que aquél resulta especialmente vulnerable, es decir, mientras la comunicación se encuentra en tránsito o en poder de un tercero encargado de su remisión o envío. La protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero una vez finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos. De ahí que, una vez concluido el proceso comunicativo, la tutela de los derechos que convergen para la protección de lo comunicado, adquiría una dimensión distinta a través del derecho a

la privacidad (art. 18.1 CE) o del derecho a la protección de datos (art. 18.4 CE). Esta doctrina fue confirmada por la STC 123/2002, 20 de mayo y, en buena medida, por la STC 173/2011 de 7 de noviembre: *«el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o e-mails, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado».* La jurisprudencia mayoritaria del Tribunal Supremo se adscribe a la tesis defendida en la STC 70/2002, 3 de abril, de suerte que, finalizada la comunicación, el contenido de lo comunicado y los datos asociados quedan fuera del ámbito de protección del art. 18.3 de la CE. Con distintos matices en función del vehículo, técnico o convencional, empleado para la comunicación[50].

3.2.3. La interceptación legal de las comunicaciones

Un aspecto fundamental es la **motivación del auto inicial** que acuerde la intervención telefónica, en este sentido la STS 158/2014 de 12 de marzo, resume los criterios doctrinales del Tribunal Constitucional y del Tribunal Supremo al respecto. En primer lugar, la resolución judicial que acuerda una intervención telefónica ha de justificar la existencia de los presupuestos materiales habilitantes de la intervención: los datos objetivos que puedan considerarse indicios de la posible comisión de un hecho delictivo grave y de la conexión de las personas afectadas por la intervención con los hechos investigados. Indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento. En este sentido, es doctrina reiterada que *«la relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal Constitucional, no son tan sólo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control y en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona. Esta mínima exigencia resulta indispensable desde la perspectiva del derecho fundamental, pues si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones, tal y como la Constitución lo configura,*

[50] SSTS 1235/2002 de 27 de junio, 1647/2002 de 1 de octubre, 1231/2003 de 25 de septiembre, 14/2008 de 18 de enero, 1273/2009 de 17 de diciembre, 1315/2009 de 18 de diciembre, 247/2010 de 18 de marzo y 266/2010 de 31 de marzo.

quedaría materialmente vacío de contenido[51]*»*. A este respecto no se trata de satisfacer los intereses de una investigación meramente prospectiva, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar sospechas sin base objetiva de los encargados de la investigación, por más legítima que sea esta aspiración, pues de otro modo se desvanecería la garantía constitucional[52]. Junto con tales datos objetivos, debe determinarse con precisión el número o números de teléfonos que deben ser intervenidos, el tiempo de duración de la intervención, quien ha de llevarla a cabo y los periodos en los que deba darse al Juez de sus resultados a los efectos de que éste controle su ejecución[53]. En todo caso y aunque es deseable que la resolución judicial contenga en sí misma todos los datos anteriores, nuestra jurisprudencia ha admitido la motivación por remisión, de modo que la resolución judicial puede considerarse suficientemente motivada si, integrada con la solicitud policial, a la que puede remitirse, contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad[54], han estimado suficiente que la motivación fáctica de este tipo de resoluciones se fundamente en la remisión a los correspondientes antecedentes obrantes en las actuaciones y concretamente a los elementos fácticos que consten en la correspondiente solicitud policial, o en su caso del Ministerio Fiscal, que el Juzgador tomó en consideración como indicio racionalmente bastante para acordar la intervención telefónica. Como señalan las SSTS de 26 de junio de 2000, 3 de abril y 11 de mayo de 2001, 17 de junio y 25 de octubre de 2002, entre otras muchas, los autos de autorización de intervenciones telefónicas pueden ser integrados con el contenido de los respectivos oficios policiales en los que se solicitan las intervenciones en cada caso, de forma que es lícita la motivación por referencia a los mismos, ya que el Órgano Jurisdiccional carece por sí mismo de la información pertinente y no sería lógico que abriese una investigación paralela al objeto de comprobar los datos suministrados por la Policía Judicial". Como se recuerda en la STC 167/2002, de 18 de septiembre, aunque lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención quede exteriorizada directamente en la resolución judicial, ésta puede considerarse suficientemente motivada si, integrada incluso con la solicitud policial, a la que puede remitirse, contiene los elementos necesarios para considerar satisfechas las

---

[51] STC 49/1999 de 5 de abril, 166/1999 de 27 de septiembre, 171/1999 de 27 de septiembre, 299/2000 de 11 de diciembre, 14/2001, de 29 de enero, 138/2001 de 18 de junio, 202/2001 de 15 de octubre, 167/2002 de 18 de septiembre, 184/2003 de 23 de octubre, 261/2005 de 24 de octubre, 220/2006 de 3 de julio, 195/2009 de 28 de septiembre y 5/2010 de 7 de abril.

[52] SSTC 184/2003 de 23 de octubre y 261/2005 de 24 de octubre.

[53] SSTC 49/1996 de 26 de marzo, 49/1999 de 5 de abril, 167/2002 de 18 de septiembre, 184/2003 de 23 de octubre, 259/2005 de 24 de octubre y 136/2006 de 8 de mayo.

[54] SSTC 167/2002 de 18 de septiembre, 184/2003 de 23 de octubre, 259/2005 de 24 de octubre y 136/2006 de 8 de mayo.

exigencias para poder llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva. Así pues, la motivación en cuanto a los hechos que justifican la adopción de la medida, debe contemplar la individualidad de cada supuesto en particular, y puede hacerlo remitiéndose a los aspectos fácticos contenidos en el oficio policial en el que se solicita su adopción. No se trata desde luego de una práctica recomendable, a pesar de la frecuencia con la que se recurre a ella, pero no determina por sí misma la nulidad de lo actuado. Asimismo el Tribunal Constitucional ha venido reconociendo cánones de suficiencia razonadora en autos con motivación "lacónica" e incluso cuando se extiende el auto sobre impresos estereotipados, mínimamente adecuados a las circunstancias del caso particular, siempre que permitan reconocer unos mínimos razonadores que den satisfacción a la exigencia constitucional, y recogiendo esta misma doctrina constitucional, el Tribunal Supremo ha venido a sostener que esta exigencia motivadora no es incompatible con una economía de razonamientos ni con una motivación concisa, escueta y sucinta, porque la suficiencia del razonamiento no conlleva necesariamente una determinada extensión, ni determinado vigor lógico o una determinada elegancia retórica (STS de 4 de marzo de 1999).

En lo referente a la interceptación legal de las comunicaciones, el artículo 83 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, regula en su capítulo II, la interceptación legal de las comunicaciones, que podría definirse como la medida establecida por ley y adoptada por una autoridad judicial que acuerda o autoriza el acceso o la transmisión de las comunicaciones electrónicas de una persona, y la información relativa a la interceptación, a los agentes facultados[55], sin perjuicio de lo establecido en el artículo 579.4 de la Ley de Enjuiciamiento Criminal. Las comunicaciones susceptibles de ser interceptadas, según el artículo 83 del Reglamento anterior, serán las dispuestas en el artículo 579 de la LECrim, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, y en otras normas con rango de ley orgánica.

La interceptación, según el art. 90 del citado Reglamento, se llevará a efecto si en la orden de interceptación legal se incluye, al menos, uno de los datos siguientes:

a) La identificación del abonado o usuario sujeto a la interceptación.

[55] Agente facultado: policía judicial o personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar una interceptación legal

b) La ubicación donde se encuentre un punto de terminación de red al que el operador da servicio.

c) Un identificador de punto de terminación de red (dirección), o de terminal, al que el proveedor de servicios de comunicaciones electrónicas da servicio.

d) El código de identificación en caso de que sea el usuario el que active el terminal para la comunicación.

e) Cualquier otra identidad (en la acepción definida en el artículo 84.i) que corresponda al sujeto especificado en la orden de interceptación legal.

El plazo de ejecución de una orden de interceptación, regulado en el artículo 99 del Reglamento, será el fijado en ella. Cuando no se establezca plazo, las órdenes se ejecutarán antes de las 12:00 horas del día laborable siguiente al que el sujeto obligado reciba la orden de interceptación legal. Cuando la orden de interceptación legal establezca la urgencia de su ejecución, los sujetos obligados deberán ejecutarla con la mayor brevedad posible teniendo en cuenta lo dispuesto en la orden de interceptación. Por aplicación analógica del artículo 579.3 de la LECRIM ha de entenderse que la orden judicial se mantiene vigente por durante un periodo de tres meses, prorrogables por igual tiempo, como norma general, ya que en el apartado 4º se establece que en caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación.

3.2.4. El programa SITEL

El programa SITEL (Sistema Integrado de Interceptación Telefónica) es el empleado para realizar las interceptaciones telefónicas, cuya titularidad ostenta el Ministerio de Interior, según este organismo, su desarrollo responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garantista para la figura o concepto jurídico de la intervención de las comunicaciones. Aunque resultan confusos los datos sobre la fecha efectiva de implantación, los orígenes se sitúan en el año 2001, cuando se comenzó a gestar el proyecto, siendo objeto de debate jurisprudencial desde 2008. Así la STS 1215/2009 de 30 de diciembre realiza un pormenorizado estudio de la adecuación a la legalidad de las escuchas telefónicas. El sistema SITEL se articula sobre tres principios de actuación:

a) **Centralización**: El servidor y administrador del sistema se encuentra en una sede central, distribuyendo la información aportada por las operadoras de comunicaciones de los distintos usuarios implicados.

b) **Seguridad**: El sistema establece numerosos filtros de seguridad y responsabilidad, apoyados en el principio anterior. Existen dos ámbitos de seguridad:
   1. Nivel central: Existe un ordenador central del sistema para cada sede reseñada, dotado del máximo nivel de seguridad, con unos operarios de mantenimiento específicos. Desde el mismo se dirige la información a los puntos de acceso periféricos de forma estanca. La misión de este ámbito central es almacenar y distribuir la información.
   2. Nivel periférico: El sistema cuenta con ordenadores para su empleo en los grupos periféricos de enlace en las Unidades encargadas de la investigación y responsables de la intervención de la comunicación, dotados de sistema de conexión con sede central propio y seguro.
   3. Se establece codificación de acceso por usuario autorizado y clave personal, garantizando la conexión al contenido de información autorizado para ese usuario, siendo necesario que sea componente de la Unidad de investigación encargada y responsable de la intervención .

c) **Automatización**: El sistema responde a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, dotándole de mayor nivel de garantía y seguridad, reduciendo costes y espacio de almacenamiento, así como adaptarse al uso de nuevos dispositivos de almacenamiento.

El sistema, en la actualidad, aporta la siguiente información relativa a la intervención telefónica:

a) Fecha, hora y duración de las llamadas.
b) Identificador de IMEI y nº de móvil afectado por la intervención.
c) Distribución de llamadas por día.
d) Tipo de información contenida (SMS, carpeta audio, etc.).
e) IMEIS correspondientes a los teléfonos intervinientes.
f) Identidad del titular de los teléfonos que interactúan aunque sean secretos.

En referencia al contenido de la intervención de la comunicación, y ámbito de información aportada por el sistema, se verifican los siguientes puntos:

a) Repetidor activado y mapa de situación del mismo.
b) Número de teléfono que efectúa y emite la llamada o contenido de la información.
c) Contenido de las carpetas de audio (llamadas) y de los mensajes de texto (SMS).

Su sistema de trabajo es el siguiente: Solicitada la intervención de la comunicación y autorizada por la Autoridad Judicial, la operadora afectada inicia el envío de información al Servidor Central donde se almacena a disposición de la Unidad encargada y solicitante de la investigación de los hechos, responsable de la intervención de la comunicación. El acceso por parte del personal de esta Unidad se realiza mediante "código identificador de usuario y clave personal". Realizada la supervisión del contenido, se actúa igual que en el modo tradicional, confeccionando las diligencias de informe correspondientes para la Autoridad Judicial.

La evidencia legal del contenido de la intervención es aportada por el Servicio Central, responsable del volcado de todos los datos, a formato DVD para entrega a la autoridad judicial competente, constituyéndose como la única versión original, facilitando su entrega por la Unidad de investigación a la autoridad judicial competente, constituyéndose como la única versión original, verificándose que en sede central no quede vestigio de la información (STS 1078/2009, de 5 de noviembre).

Pese al intenso debate sobre la validez legal al empleo de la herramienta SITEL, se ha aceptado mayoritariamente su legalidad, en base a todo ello, la STS 722/2012 de 2 de octubre y siguiendo la STS 554/2012, de 4 de julio, entiende que ningún reparo cabe hacer al empleo de esta tecnología informática. Como señala la STS 573/2012, *«ha de recordarse que, tras un intenso debate acerca del sistema SITEL, la mayoría de esta Sala ha considerado dicho modo de proceder como técnicamente fiable, por encima incluso del sistema "tradicional" de grabación de esas comunicaciones»*. Y en la sentencia 410/2012, de 17 de mayo, se señala que la posibilidad de manipulación o alteración del resultado de las intervenciones en el sistema SITEL es prácticamente imposible. Cuando el Juez ordena una intervención telefónica no impone la utilización de ningún sistema, sino que autoriza los más avanzados o los que en un momento dado utilice la policía judicial, siempre que ofrezcan plenas garantías, como sucede con el sistema SITEL según la doctrina jurisprudencial anteriormente citada, que es el que se ha incorporado con carácter general en nuestro ordenamiento. En consecuencia, si la doctrina jurisprudencial ya ha estimado que, con carácter general, el sistema SITEL ofrece suficientes garantías para la validez probatoria de las intervenciones que lo utilicen, y teniendo en cuenta que es el sistema de uso habitual en todos los procedimientos judiciales, resulta innecesaria la práctica de una compleja y dilatoria prueba pericial informática para conocer o acreditar las características básicas del

sistema, en todos y cada uno de los juicios que se celebran en los que se aporten como prueba dichas intervenciones.

En nuestro ordenamiento, la principal garantía para la validez constitucional de una intervención telefónica es, por disposición constitucional expresa, como señala la STS 722/2012 de 2 de octubre, *«la exclusividad jurisdiccional de su autorización, lo que acentúa el papel del Juez Instructor como Juez de garantías, ya que lejos de actuar en esta materia con criterio inquisitivo impulsando de oficio la investigación contra un determinado imputado, la Constitución le sitúa en el reforzado y trascendental papel de máxima e imparcial garantía jurisdiccional de los derechos fundamentales de los ciudadanos. De esta manera en la investigación, impulsada por quienes tienen reconocida legal y constitucionalmente la facultad de ejercer la acusación, no se puede, en ningún caso ni con ningún pretexto, adoptar medidas que puedan afectar a dichos derechos constitucionales, sin la intervención absolutamente imparcial del Juez, que en el ejercicio de esta función constitucional, que tiene atribuida con carácter exclusivo, alcanza su máxima significación de supremo garante de los derechos fundamentales»*. Para la validez constitucional de esta medida de intervención telefónica es necesario que concurran los siguientes elementos: a) resolución judicial, b) suficientemente motivada, c) dictada por Juez competente, d) en el ámbito de un procedimiento jurisdiccional, e) con una finalidad específica que justifique su proporcionalidad, f) judicialmente controlada en su desarrollo y práctica. Elementos que constituyen los presupuestos legales y materiales de la resolución judicial habilitante de una injerencia en los derechos fundamentales, y que también se concretan en la doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos. En relación con el requisito de la motivación es doctrina reiterada del Tribunal Supremo y del Tribunal Constitucional que constituye una exigencia inexcusable por la necesidad de justificar el presupuesto legal habilitante de la intervención (STC 253/2006, de 11 de septiembre), y que en el momento inicial del procedimiento en el que ordinariamente se acuerda la intervención telefónica no resulta exigible una justificación fáctica exhaustiva, pues se trata de una medida adoptada, precisamente, para profundizar en una investigación no acabada[56], por lo que únicamente pueden conocerse unos iniciales elementos indiciarios. Es por ello por lo que tanto el Tribunal Constitucional como la Sala Segunda del Tribunal Supremo[57] han estimado suficiente que la motivación fáctica de este tipo de resoluciones se fundamente en la remisión a los correspondientes antecedentes obrantes en las actuaciones y concretamente a los elementos fácticos que consten en la correspondiente solicitud policial, o en el informe

[56] SSTS 1240/98 de 27 de noviembre, 1018/1999 de 30 de septiembre, 1060/2003 de 21 de julio, 248/2012 de 12 de abril y 492/2012 de 14 de junio, entre otras.

[57] SSTC 123/1997 de 1 de julio, 165/2005 de 20 de junio, 26/2006 de 30 de enero y 146/2006 de 8 de mayo.

o dictamen del Ministerio Fiscal, cuando se ha solicitado y emitido (STS 248/2012, de 12 de abril).

La importancia de respetar todos los requisitos y de ajustar el procedimiento a las exigencias legales resulta evidente; la STS 100/2014 de 18 de febrero hace una exposición clara sobre sus efectos, y así, en principio, los datos que se hayan obtenido en una investigación realizada sobre la base de lo conocido en unas escuchas telefónicas acordadas vulnerando el derecho fundamental al secreto de esa clase de comunicaciones, no podrán ser empleados legítimamente como pruebas o para obtener pruebas, aunque éstas, en si mismas y aisladamente consideradas, hayan sido obtenidas sin vulneración de derecho alguno[58]. Así, los datos obtenidos en una intervención telefónica que vulnera el derecho al secreto de las comunicaciones, no pueden ser, pues, utilizados para justificar válidamente otra intervención o una entrada y registro de las que se obtienen pruebas del delito, aun cuando estas segundas no comporten en sí mismas ninguna vulneración de derechos. Del mismo modo, el conocimiento exclusivamente obtenido a través de las escuchas constitucionalmente ilícitas respecto de la existencia de datos sobre la base de los que se construye la sospecha sobre personas hasta ese momento desconocidas o no sospechosas, no permite considerar válida la investigación realizada sobre éstas o la adopción de medidas restrictivas de sus derechos.

3.3. REGISTROS E INVIOLABILIDAD DE DOMICILIO (ART. 18.2 CE)

Otro derecho que puede vulnerarse en la obtención de este tipo de pruebas es el contenido en el artículo 18.2 CE, la inviolabilidad de domicilio, no pudiendo realizarse

[58] STS 811/2012 de 30 de octubre: *«el Tribunal Constitucional ha establecido una doble perspectiva de análisis: una perspectiva interna, que atiende a la índole y características de la vulneración del derecho constitucional violado; en el caso, al secreto de las comunicaciones en la prueba originaria (qué garantías de la injerencia en el derecho se han visto menoscabadas y en qué forma), así como al resultado inmediato de la infracción (el conocimiento adquirido a través de la injerencia practicada inconstitucionalmente). Por otro lado, una perspectiva externa, que atiende a las necesidades esenciales de tutela que la realidad y efectividad del derecho conculcado exige. En cuanto al resultado se ha precisado que debe valorarse si el dato obtenido de la diligencia ilícita hubiera podido obtenerse normalmente, dadas las concretas circunstancias, por medios distintos, lícitos e independientes; o si se trata de un dato de significado tan neutro que solo alcanza valor tras la realización de una investigación que pudiera haberse iniciado de forma independiente de su obtención, dadas las sospechas ya formuladas. Y en cuanto a las necesidades de tutela del derecho se ha mencionado especialmente la índole del derecho vulnerado y la entidad de la vulneración, así como la existencia de dolo o intención de vulnerar el derecho, aunque sea este último un aspecto más propio de ordenamientos anglosajones. En todo caso ha de tenerse en cuenta que la concurrencia de mala fe en la actuación policial o judicial suprime cualquier disminución en la necesidad de tutela del derecho fundamental afectado, la cual, precisamente, debe ser reforzada en esos casos, lo que impediría considerar la existencia de un supuesto de desconexión jurídica a los efectos que se examinan».*

ninguna entrada o registro sin el consentimiento del titular o resolución judicial, excepto en el caso de flagrante delito.

Normalmente los equipos informáticos se encuentran en un lugar cerrado, por lo que es necesaria la intervención judicial como recoge el artículo 546 LECRIM *«cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación»*; y como resultaría lógico, la orden de entrada y registro conllevaría en estos casos también la incautación de los medios informáticos, en este sentido la STS 342/2013 de 17 de abril, señala:

> ***«****Carecería de todo sentido que la autorización judicial se limitara a facultar a los agentes a la práctica de una inspección ocular que les permitiera "averiguar" la existencia de los equipos técnicos desde los que se estaba cometiendo graves delitos contra menores y que, una vez averiguada esa existencia, se obligara a los agentes a marcharse del domicilio registrado, dejando esos elementos de prueba de primer orden en poder del imputado. No cabe duda alguna de que esa averiguación sólo adquiere sentido como medio para, una vez constatada su existencia, intervenir lo que, como exponía la solicitud policial no eran sino instrumentos de graves delitos para cuyo esclarecimiento se había concedido, precisamente, el mandamiento de entrada y registro. En definitiva, desde este punto de vista, es claro que para "averiguar" si los ordenadores y demás dispositivos intervenidos tenían o no relación con el delito que estaba siendo objeto de investigación, resultaba indispensable su intervención y, claro es, su ulterior examen».*

El artículo 569 de la LECRIM, en garantía del derecho de defensa establecido en el artículo 24 CE, establece que el registro se realizará en presencia del interesado o persona que legalmente le represente, y estando siempre presente el Secretario judicial. Sobre la posibilidad de intervención letrada, la STS 77/2014 de 11 de febrero es clara:

> ***«****Respecto de la presencia de Letrado en la práctica de la diligencia de entrada y registro, la jurisprudencia de esta Sala es unánime al respecto. En efecto, la STS 697/2003, de 16 de mayo, citando la STS 1116/98, 30 de septiembre, razona que "la intervención de letrado en los registros domiciliarios no es exigida ni por el artículo 17.3 de la Constitución ni por los Pactos Internacionales suscritos por España, estando circunscrita como obligatoria tan sólo para las declaraciones prestadas por el imputado y en los reconocimientos de identidad de que él mismo sea objeto. En consecuencia, la no asistencia letrada al registro practicado en los domicilios del recurrente no constituyó infracción de su derecho a un proceso con todas las garantías, habiéndose dado cumplimiento a las exigencias constitucionales de resolución judicial motivada así como a las de la legislación ordinaria que la desarrollan". Esta idea es*

reiterada en otros muchos pronunciamientos que destacan cómo la asistencia letrada se circunscribe a la práctica de diligencias de carácter personal, en los términos a que se refiere el artículo 520 de la Ley de Enjuiciamiento Criminal, sin afectar a la diligencia de entrada y registro (cfr., por todas SSTS 953/2010, 27 de octubre; 1134/2009, 17 de noviembre y ATS 599/2010, 17 de junio)».

La forma habitual de obtener la información contenida en un medio informático es la incautación del equipo tras una orden de entrada y registro en un domicilio, resultando imprescindible la asistencia de un especialista informático que evite que se pierda o destruya información y evitar además inspecciones inútiles, procurando no perjudicar ni importunar al interesado, como así recoge el artículo 552 LECRIM. En otros casos, no es necesaria la incautación del ordenador, pudiendo adquirirse la información contenida en el mismo mediante el clonado o volcado técnico del contenido del disco duro en una réplica con las copiadoras, con la práctica del oportuno *resumen digital hash*, garantizando la presencia del Secretario judicial la operación con su supervisión jurídica, y una vez finalizada, cerrará con el precinto el disco duro original, cediendo copia clonada a los peritos. Como apunta VELASCO NUÑEZ[59] el clonado o volcado del disco duro es una operación de copiado de la información tal y como obraba en el disco duro del ordenador al momento de la entrada y registro, que en realidad virtual es algo equivalente a lo que en soporte papel suponen las fotocopias o en el audio las copias de CD, y en el video las de DVD. Es una garantía de lo que se copia es exacto de lo que se ocupa, asegurando la integridad del contenido y su no alterabilidad; por tanto se mantiene la cadena de custodia mediante el copiado en modo de solo lectura y por tanto no modificable y se verifica contrastando el resumen digital recogido sobre la prueba original , basado en algoritmos *hash*, con el de la copia analizada, que se entregará a los peritos, quedando el original custodiado por el Secretario judicial, garantizado que el objeto de la pericia es el mismo que el aprehendido y analizado.

La apertura del disco duro ha de realizarse en presencia igualmente del Secretario judicial, como así se desprende de los artículos 567 y 570 LECRIM, constituyendo su presencia así como la autorización judicial de la entrada y registro los requisitos básicos del derecho a un proceso con todas las garantías, en este sentido, SAP de Huelva, sección 3ª rec. 87/2012 de 22 de junio de 2012:

---

[59] VELASCO NUÑEZ, E. en su artículo *"Pericias informáticas: aspectos procesales penales"* en I CONGRESO CIENTÍFICO DE LA ABOGACÍA DEL PRINCIPADO DE ASTURIAS. *"Libro de ponencias",* op. cit., (pp. 135 a 158).

«Como motivo segundo alega violación de garantías constitucionales con motivo del irregular proceder en la aprehensión de la evidencia probatoria durante el operativo de entrada y registro, al no haberse realizado una inspección sobre el equipo sino simplemente mera aprehensión y registro de la carcasa exterior y número del equipo, no del disco duro, ni examen de sus componentes. En primer lugar, debe señalarse que la irregularidad que señala el recurrente no supondría -de existir- ninguna infracción de orden constitucional bajo la que se cobija el motivo. El registro efectuado será constitucionalmente legítimo siempre que se produzca con consentimiento del afectado libremente expresado, o, en su defecto, mediante autorización judicial debidamente motivada. A partir de aquí, las deficiencias o irregularidades que se produzcan en la ejecución de dicha diligencia carecerán de relevancia constitucional y lo serán únicamente de legalidad ordinaria. En definitiva, no existió una vulneración del derecho a un proceso con todas las garantías, pues autorizada judicialmente la entrada y registro (folios 56 y 57) la misma se realizó a presencia del secretario judicial (folio 59 y ss). El agente NUM000 que intervino en la entrada y registro manifestó en el plenario que una vez en la gestoría, hicieron un examen de los ordenadores interviniendo el que se encontraba en el despacho del acusado y en el acta de entrada y registro se detalla el lugar en el que fue intervenida la torre (el despacho del acusado), haciéndose constar igualmente que el motivo por el que no fueron intervenidos el resto de los ordenadores fue por no encontrar nada de interés en los mismos».

Un aspecto sustancial que no vulnere este derecho así como otras garantías constitucionales, es la correcta fundamentación del auto de entrada y registro que justifique la adopción de esta medida. Así lo recoge la STS 654/2013 de 26 junio:

«Entre los presupuestos comunes está tanto la autorización judicial, como la calidad de esta; en una doble vertiente que constituye como el anverso y reverso de una misma realidad: ha de tratarse de una resolución fundada en el sentido tanto externo (motivada) como intrínseco o interno (con fundamento). La primera faceta será muestra de la segunda. No basta con una motivación formal (que por otra parte puede cubrirse con una remisión al material que sirve de antecedente): no estamos ante un simple rito. No basta una fundamentación teórica o estereotipada o genérica. Lo relevante es la fundabilidad material en concreto: que existan "buenas razones" para el alzamiento de ese derecho de rango fundamental. Para que sea constitucionalmente legítima la suspensión del derecho a la inviolabilidad del domicilio, el Juez ha de verificar la presencia de indicios objetivables. Meras afirmaciones apodícticas de sospecha no la pueden justificar. El órgano judicial ha de valorar no sólo la gravedad y naturaleza de los delitos que se pretende indagar; y la necesidad de la invasión de un derecho fundamental para preservar las finalidades de la investigación. Es imprescindible un juicio ponderativo judicial sobre el nivel cualificativo de los indicios que avalan las sospechas. La suficiencia de los indicios para llegar a afirmar la probabilidad de esas conclusiones es una valoración que no puede hurtarse al Juez de Instrucción: no puede descansar exclusivamente

en los agentes policiales. No basta con que éstos afirmen que tienen sospechas fundadas. Es necesario que aporten al instructor los elementos objetivos que apoyan ese juicio de probabilidad. No es suficiente una intuición policial; ni una sospecha más o menos vaga; ni deducciones basadas únicamente en confidencias. El éxito posterior de la investigación, no sirve para convalidar lo que en sus raíces nacía podrido: se trata de un juicio ex ante[60]. Solo está legal y constitucionalmente legitimada una decisión judicial de la naturaleza de la analizada cuando hubiere indicios de encontrarse allí (en la vivienda) el procesado o efectos e instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento o comprobación (arts. 546 y 550 LECRIM)».

El auto de entrada y registro[61] ha de precisar los indicios racionales en que se asienta como previos a la valoración de los intereses en juego, no siendo suficiente las meras sospechas o conjeturas, así como respetar los requisitos de proporcionalidad y necesidad para la adopción de la medida. Un aspecto controvertido es la remisión al al oficio policial interesando mandamiento de entrada y registro, para integrar el auto habilitante, posibilidad aceptada por la jurisprudencia constitucional y del Tribunal Supremo, siempre que conste o se infiera, que el juez ha tenido conocimiento pleno de tal oficio y lo ha valorado.

3.4. DERECHO A LA INTIMIDAD (ART. 18.1 CE)

El artículo 18.1 CE garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, guardando estrecha relación con el artículo 20.4 del texto constitucional, que dispone que el respeto a tales derechos constituirá un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales. Su desarrollo legislativo está contenido en la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento.

Como distingue la SAP de Logroño, Secc.1ª, 55/2014 de 21 de febrero, los derechos al honor, a la intimidad y a la imagen son tres derechos distintos y no un solo derecho

[60] SSTC 165/2005 de 20 de junio y 259/2005 de 24 de octubre.

[61] STS 785/2008 de 25 de noviembre.

trifronte[62], sin que quepa mezclarlos ni confundirlos[63], *«se trata de derechos que tienen en nuestro ordenamiento sustantividad y contenido propio, de modo que ninguno queda subsumido en el otro, como si fuera una manifestación concreta de él[64]. Lo que implica admitir la posibilidad de que unos mismos actos constituyan intromisión ilegítima en el ámbito de protección reconocido a todos o sólo a alguno de ellos. Se hace indispensable, por lo tanto, poner en relación las circunstancias concurrentes con cada uno de esos derechos -honor, intimidad personal y propia imagen-, considerando cuáles son sus contenidos respectivos y cuáles los límites que les afectan e interesan al caso».*

El artículo 18.1 CE garantiza el derecho al honor[65] como una de las manifestaciones de la dignidad de la persona, proclamada en el artículo 10 CE . Su precisión[66] depende de las normas, valores e ideas sociales vigentes en cada momento, y presenta, según consolidada doctrina jurisprudencial, una doble dimensión, objetiva y subjetiva, si bien el ámbito de protección constitucional y jurisdiccional se extiende verdaderamente, no a la autoestima, consideración propia o idea que uno tiene de sí mismo (inmanencia), sino a la reputación, heteroestima o consideración que de uno tienen los demás (trascendencia o valoración social), impidiendo la difusión de expresiones o mensajes insultantes, insidias infamantes o vejaciones que provoquen objetivamente el descrédito. En esta línea, la reciente STS 18 de febrero de 2013, Rec. 1229/2011[67] declara que *«El artículo 7.7 LPDH define el derecho al honor en un sentido negativo, desde el punto de vista de considerar que hay intromisión por la imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación»*. Doctrinalmente se ha definido como dignidad personal reflejada en la consideración de los demás y en el sentimiento de la propia persona. Según reiterada jurisprudencia (SSTS de 16 de febrero de 2010 y 1 de junio de 2010) *«es preciso que el honor se estime en un doble aspecto, tanto en un aspecto interno de íntima convicción - inmanencia- como en un aspecto externo de valoración social -trascendencia-, y sin caer en la tendencia doctrinal que proclama la minusvaloración actual de tal derecho de la personalidad».* Como ha señalado

---

[62] STS 26 de febrero de 2009, Rec. 958/2006 y 31 de marzo de 2010, Rec. 2118/2007.

[63] STS 24 de julio de 2012, Rec. 355/2011.

[64] SSTC 81/2001 de 26 de marzo , y 156/2001 de 2 de julio.

[65] STS194/2014 de 3 de enero.

[66] SAP de la Rioja Nº 55 de 2014 de 21 de febrero.

[67] También las SSTS de 21 de enero de 2013, Rec. 26/2009 y 5 de febrero de 2013, Rec. 1255/2011.

reiteradamente el Tribunal Constitucional[68] el honor constituye un *«concepto jurídico normativo cuya precisión depende de las normas, valores e ideas sociales vigentes en cada momento»*. Este Tribunal ha definido su contenido afirmando que este derecho protege frente a atentados en la reputación personal entendida como la apreciación que los demás puedan tener de una persona, independientemente de sus deseos (STC 14/2003, de 28 de enero), impidiendo la difusión de expresiones o mensajes insultantes, insidias infamantes o vejaciones que provoquen objetivamente el descrédito de aquélla (STC 216/2006, de 3 de julio). La STS 1 de marzo de 2010, con cita de las de 17 de febrero de 2009 y 16 de julio de 2009, recuerda que *«el honor tiene un sentido subjetivo y un sentido objetivo; el primero es el sentimiento de la propia persona, en su consideración personal, la inmanencia, representado por la estimación que cada persona hace de sí mismo y el segundo es la trascendencia o exteriorización, representado por la estimativa que los demás hacen de nuestra dignidad».*

El derecho al honor, según reiterada jurisprudencia, se encuentra limitado por las libertades de expresión e información. La limitación del derecho al honor por la libertad de información o de expresión tiene lugar cuando se produce un conflicto entre uno y otro derecho, el cual debe ser resuelto mediante técnicas de ponderación constitucional, teniendo en cuenta las circunstancias del caso[69]. Por ponderación se entiende, tras la constatación de la existencia de una colisión entre derechos, el examen de la intensidad y trascendencia con la que cada uno de ellos resulta afectado, con el fin de elaborar una con el fin de elaborar una regla que permita, dando preferencia a uno u otro, la resolución del caso mediante su subsunción en ella.

El derecho a la intimidad, igualmente recogido en el artículo 18.1 CE, está directamente relacionado con el derecho al secreto de comunicaciones, con el que a veces se confunde. A este respecto, señala la STS 785/2008 de 25 de noviembre:

> *«La Audiencia distinguió con acierto entre "comunicación ex novo" y "comunicación concluida", al recoger la doctrina consolidada del Tribunal Constitucional, lo que supondría un distinto régimen jurídico. La propia sentencia invocada por el recurrente al aludir a las características delimitadoras del secreto protegido en el art. 18.3 distingue entre la intimidad personal que tendría su adecuado cobijo en el art. 18.1 y el secreto de las comunicaciones art. 18.3 CE. Se viene a dejar sentado que si "ex art. 18.3 C.E." la intervención de las*

[68] SSTC 180/1999 de 11 de octubre, 52/2002 de 25 de febrero y 51/2008 de 14 de abril.

[69] SSTS de 12 de noviembre de 2008, RC n.º 841/2005, 19 de septiembre de 2008, RC n.º 2582/2002, 5 de febrero de 2009, RC n.º 129/2005, 19 de febrero de 2009, RC n.º 2625/2003, 6 de julio de 2009, RC n.º 906/2006, 4 de junio de 2009, RC n.º 2145/2005, 22 de noviembre de 2010, RC nº 1009/2008 y de 1 de febrero de 2011, RC n.º 2186/2008.

comunicaciones requiere siempre resolución judicial, "no existe en la Constitución reserva absoluta de previa resolución judicial" respecto del derecho a la intimidad personal, de modo que excepcionalmente se ha admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad. En nuestro caso se trataba de unas comunicaciones por Internet, ya celebradas y concluidas, de tal suerte que sólo constituía material de archivo. La Audiencia Provincial entiende y lo hace con acierto que el auto de entrada y registro comprende esta diligencia, por cuanto a la vista de la naturaleza del delito que se investigaba la policía estaba autorizada a recoger los objetos o instrumentos de los que pudiera deducirse la comisión del delito y que fueran hallados en el recinto registrado, y en este sentido se intervienen los ordenadores y su disco duro. No fueron los mismos policías los que realizaron el volcado, resultando lógico encomendarlo a la policía judicial experta en estas materias, a cuyo efecto fueron designados otros policías peritos, los cuales por providencia del juez instructor la llevaron a cabo responsablemente (providencia de 3 de junio de 2005, folio 157 de las actuaciones). Así pues, aunque había bastado el auto inicial, en el que no existe ninguna cortapisa en cuanto se trate de intervenir objetos o instrumentos o en general piezas de convicción que acrediten la comisión del delito investigado, la policía hizo una razonable y prudente interpretación del auto, sin excederse lo más mínimo de lo que constituía el propósito de la diligencia ordenada. La posterior providencia sólo tuvo por causa la exigencia de que la operación de volcado la efectuasen expertos de la policía».

3.4.1. Obtención de la dirección I.P.

En muchas ocasiones, como señala VELASCO NÚÑEZ[70] tras el rastreo policial en Internet se obtienen las señas IP vinculadas al ataque investigado, o en caso de que haya denuncia previa de una víctima, podría proporcionarlas desde el propio ordenador del denunciante, pero la obtención de los datos asociados a la dirección IP requeriría intervención judicial, ya que son datos reservados y protegidos por la Ley[71] que la empresa prestadora de servicios de Internet (ISP) tiene obligación de conservar y ceder previa autorización judicial. Aunque como señala la STS 16/2014 de 30 de enero, cuestión distinta será en los supuestos en los que en las diligencias de investigación desarrolladas por las Fuerzas y Cuerpos Policiales en la persecución de actividades delictivas de cualquier

[70] VELASCO NUÑEZ, E. en su artículo *"Pericias informáticas: aspectos procesales penales"* en I CONGRESO CIENTÍFICO DE LA ABOGACÍA DEL PRINCIPADO DE ASTURIAS. *"Libro de ponencias",* op. cit., (pp. 135 a 158).

[71] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

naturaleza para cuyo progreso sea necesario conocer el IP (o el número telefónico) de una determinada persona que hasta el momento es desconocido, se tenga que acatar esa exigencia legal. No obstante la STS 292/2008, con cita de la STS 1797/2007 de 9 de mayo, ya advertida que la complejidad de la materia, su ductilidad, y las singulares características de la normativa que la regula, hace necesario que futuras resoluciones vayan perfilando un cuerpo de doctrina atendiendo a las peculiaridades de cada caso en concreto. En esta dirección, la STS 842/2010 en un caso en que los agentes policiales rastrearon distintas IPs, cuya numeración determinaron, y con posterioridad solicitaron autorización judicial, que les fue concedida, para acceder a la identidad de los usuarios, destaca como la jurisprudencia del Tribunal supremo[72], ha señalado que en esta materia se debe concluir, en primer lugar, que los rastreos que realizan en estos casos los agentes policiales tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los *hash* que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada queda registrada siempre y ello lo sabe el usuario. Y, en segundo lugar, que, de acuerdo con la legalidad citada en las referidas Sentencias, se hace preciso, sin embargo, acudir a la autorización del juez instructor para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal. Por último la STS 342/2013 de 17 de abril, destaca la razón la defensa cuando exige todas la cautelas precisas para la cesión de los datos que debían llevar a la identificación del usuario de dos determinadas cuentas del programa de mensajería instantánea ofrecido por Microsoft. Esa información, pese a su aparente neutralidad técnica, es susceptible de protección en el ámbito de la LO 15/1999, 13 de diciembre, de Protección de Datos Personales, conviene recordar que, conforme a su art. 3, dato personal es *«cualquier información concerniente a personas físicas identificadas o identificables»*. Y para despejar cualquier duda, el art. 5 del Decreto 1720/2007, 21 de diciembre, incluye en el concepto de dato personal *«cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables»*. El carácter de la dirección IP como dato personal ha sido reconocido por la jurisprudencia del Tribunal Supremo en numerosas sentencias (SSTS 249/2008 de 20 de mayo, 236/2008 de 9 de mayo, 680/2010 de 14 de julio y 292/2008 de 28 de mayo), bien entendido que las claves identificativas IPs no concretan a la persona del usuario, sino sólo el ordenador que se ha usado, lo que hace necesario para poder llegar al ulterior conocimiento del número de teléfono y titular del contrato la posterior autorización judicial.

[72] Entre otras, STS 739/2008 de 12 de noviembre.

3.4.2. Agenda de contactos de teléfono móvil

La STC 142/2012 de 2 de julio analiza la cuestión de si el acceso a la agenda del teléfono móvil de una persona es un acto administrativo sólo con incidencia en el derecho a la intimidad (art. 18.1 CE) o alcanza también al derecho al secreto de las comunicaciones (art. 18.3 CE), lo que, en última instancia, tiene relevancia por el diferente régimen constitucional de protección de ambos derechos. A esos efectos, cabe recordar que el Tribunal Constitucional ha señalado que si bien, de conformidad con el art. 18.3 CE, la intervención de las comunicaciones requiere siempre resolución judicial, no existe en el art. 18.1 CE esa misma garantía de previa resolución judicial respecto del derecho a la intimidad personal, de modo que excepcionalmente se ha admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad[73]. También ha reiterado que el derecho al secreto de las comunicaciones (art. 18.3 CE) consagra la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado tanto por la interceptación en sentido estricto –aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación del proceso de comunicación– como por el simple conocimiento antijurídico de lo comunicado –apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil, por ejemplo–. Igualmente se ha destacado que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores, por lo que queda afectado por este derecho tanto la entrega de los listados de llamadas telefónicas por las compañías telefónicas como también el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil[74]. Por su parte, en lo que se refiere al derecho a la intimidad (art. 18.1 CE), es doctrina constitucional que la apertura de una agenda y la lectura de los papeles que se encontraban en ella inciden en el derecho a la intimidad (STC 70/2002 de 3 de abril). Igualmente, se ha puesto de manifiesto que, a pesar de las múltiples funciones tanto de recopilación y almacenamiento de datos como de comunicación con terceros a través de internet que posee un ordenador personal, el acceso a su contenido podrá afectar bien al derecho a la intimidad personal (art. 18.1 CE), bien al derecho al secreto de las comunicaciones (art. 18.3 CE) en función de si lo que resulta desvelado a terceros son,

[73] Por todas, STC 281/2006 de 9 de octubre.

[74] Por todas, STC 230/2007 de 5 de noviembre o SSTEDH de 2 de agosto de 1984, caso Malone c.Reino Unido, § 84 y, entre las últimas, de 3 de abril de 2007, caso Copland c. Reino Unido, § 43.

respectivamente, datos personales o datos relativos a la comunicación (STC 173/2011, de 7 de noviembre).

Resuelve el caso la citada STC 142/2012 de 2 de julio del siguiente modo:

> ***«****En el presente caso, atendiendo estrictamente a lo declarado probado en las resoluciones judiciales impugnadas (…)de que el acceso de los agentes de la Guardia Civil al teléfono móvil de la coimputada se limitó a los datos recogidos en el archivo de contactos telefónicos pero no en el registro de llamadas efectuadas y/o recibidas, debe concluirse que dichos datos no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación pretéritos o futuros. En efecto, con el acceso a la agenda de contactos telefónicos la Guardia Civil no ha obtenido dato alguno concerniente a la transmisión de comunicación emitida o recibida por el teléfono móvil, sino únicamente un listado de números telefónicos introducidos voluntariamente por el usuario del terminal sobre los que no consta si han llegados a ser marcados. Por tanto, siendo lo determinante para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE, en los términos ya expuestos, no el tipo de soporte, físico o electrónico, en el que la agenda de contactos esté alojada o el hecho, destacado por el recurrente, de que la agenda sea un aplicación de un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se accede, no cabe considerar que en el presente caso la actuaciones de los agentes de la Guardia Civil supusiera una injerencia en el ámbito de protección del art. 18.3 CE. A pesar de lo anterior no puede dejar de destacarse, como ya se hiciera en la citada STC 173/2011, F. 3, respecto de un ordenador personal, la circunstancia indubitada de que un teléfono móvil, al menos en este caso, es un instrumento cuyo fin esencial es la participación en un proceso comunicativo protegido por el art. 18.3 CE y, por tanto, que en el mismo quedan almacenados datos relevantes que afectan al secreto de las comunicaciones. De ese modo, la potencial afectación que el acceso a un teléfono móvil puede tener en el derecho al secreto de las comunicaciones implica que el parámetro de control a proyectar sobre la conducta de acceso a dicho instrumento deba ser especialmente riguroso, tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la Ley, como desde la perspectiva de si la concreta actuación desarrollada al amparo de dicha Ley se ha ejecutado respetando escrupulosamente el principio de proporcionalidad».*

En la SAP de Madrid Secc. 17, 1260/2012 de 1 octubre se analiza el hecho de observar espontáneamente una llamada identificada con un nombre de contacto, en la pantalla de un teléfono móvil de un detenido, por funcionarios de la Guardia Civil. Conforme a la doctrina constitucional, considera que no constituye este hecho una injerencia ilegítima al secreto de las comunicaciones, dado que tales llamadas no fueron contestadas; en todo caso este hecho podría afectar a la intimidad, aunque tal conocimiento por parte de los

agentes se produce de forma espontánea y necesaria ante la obligación de la Guardia Civil de incomunicar al detenido y, consecuentemente, a impedirle tener a su disposición el teléfono móvil. En cambio, esta sentencia, sí considera que supone una intervención de las comunicaciones el posterior acceso que tuvieron los agentes de la Guardia Civil al contenido de las aplicaciones del teléfono móvil del detenido, accediendo al contenido de las conversaciones mantenidas por el detenido mediante la aplicación Whatsapp, lo que sí que entiende que afecta al derecho constitucional al secreto de las comunicaciones protegido en el artículo 18.3 de la Constitución. Pero tal intervención operó previa autorización judicial llevada a cabo por auto judicial, constando la información obtenida del referido terminal, en concreto, de la aplicación Whatsapp, el contenido de las conversaciones -escritas- mantenidas entre el imputado y un contacto identificado, figurando las fotografías de los "pantallazos" del terminal de teléfono. Por lo tanto, concluye, la injerencia en tal comunicación, previa autorización judicial, es legítima y por lo tanto, sin vulneración "ilegítima" de los derechos fundamentales, por lo que no cabe apreciar causa de nulidad y consideramos que tales elementos probatorios son válidos, lícitos y legítimos, susceptibles de plena valoración a la hora de enjuiciar los hechos objeto de acusación.

3.4.3. Protección de los mensajes SMS

La STS 884/2012 de 8 noviembre considera constitucionalmente protegido el contenido de los mensajes SMS, con fundamento en el art. 2.h) de la Directiva 2002/58 CE, 12 de julio, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, proporciona un concepto legal de correo electrónico, definido como *«todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo»*. A la vista de esa delimitación conceptual no puede existir duda alguna acerca de la catalogación del mensaje SMS como correo electrónico. Es cierto que no todos los contenidos imaginables de mensajería mediante teléfono móvil pueden aspirar al mismo grado de protección constitucional. No faltan casos en que el SMS se utiliza con una finalidad distinta a la transmisión de un pensamiento o de una imagen. Pensemos en su extendida utilización como forma de aviso, de comunicación, de participación en concursos, como receptor de alarmas o de titulares de un medio de comunicación. Pero lo que no es cuestionable -más allá de los matices que podrían hacerse en función del momento en el que se produce la injerencia, si ésta tiene lugar cuando el texto ya ha sido leído y simplemente está archivado- es que el mensaje de texto (*Short Message System*) entra de lleno en el contenido de la inviolabilidad de las comunicaciones. También participa de la misma naturaleza el MMS (*Multimedia Messaging System*), esto es, el mecanismo técnico

que permite el envío de imágenes entre teléfonos móviles. Sin embargo, uno cosa es el contenido de las llamadas y de los mensajes SMS y otra bien distinta el historial de esas mismas comunicaciones, como señala la sentencia.

4. CONSIDERACIONES FINALES

A fecha de finalización del presente trabajo, el Tribunal de Justicia de la Unión Europea ha dictado su sentencia en los asuntos acumulados C-293/12 y C-594/12 (Digital Rights Ireland y Seitlinger y otros), por la que anula la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, por considerar que constituye *«una injerencia de gran magnitud y especial gravedad»* en los derechos fundamentales a la privacidad y a la protección de datos de carácter personal. Asimismo, entiende que el hecho de que la conservación y la ulterior utilización de esos datos se realice sin que el abonado o el usuario registrado sea informado de ello puede generar un sentimiento de vigilancia constante en las personas. Entiende el TJUE que la obligación impuesta de conservación de datos que impone la Directiva anulada, para su posible transmisión a las autoridades competentes, responde a un objetivo de interés general, como lo es la lucha contra la delincuencia y en definitiva la seguridad pública, sin embargo, tal obligación de conservación sobrepasa los límites que exige el principio de proporcionalidad, por entender que la injerencia en los derechos fundamentales de que se trata es de gran magnitud y especial gravedad, no estando suficientemente regulada para garantizar que dicha injerencia se limita a lo estrictamente necesario.

Esta no es la única novedad que atañe a las NN.TT. y a los medios probatorios o a la investigación de delitos, dado que se prevén una serie de modificaciones en el Anteproyecto de la Ley de enjuiciamiento Criminal, como se explica en la Exposición de Motivos: *«Las disposiciones en materia de registros, aparte de introducir novedades como la regulación del registro de vehículos, responden también a la aludida voluntad de adaptación al nuevo contexto tecnológico. En este punto, al tradicional registro de libros, papeles, efectos y documentos, en el que se introduce una regulación particularizada de las cartas personales, diarios íntimos y efectos equivalentes, se añade ahora el régimen de intromisión en ordenadores, dispositivos electrónicos y sistemas de almacenamiento masivo de memoria. En todos estos casos, en defecto del consentimiento del titular, se hace necesaria la autorización del Juez de Garantías para acceder al contenido del soporte»*. Este cambio se materializa en los nuevos artículos 347 y 348, que regulan el registro e incautación de datos y archivos informáticos así como el acceso al contenido.

Otro cambio destacable que incluye el Anteproyecto de LECRIM que afecta a la materia tratada es la interceptación de comunicaciones, aunque tal vez deba revisarse tras la anulación de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas. Como señala la Exposición de Motivos, *«La nueva regulación no se refiere exclusivamente a las escuchas telefónicas, siendo aplicable a cualquier intervención de comunicaciones realizadas a través de tecnologías de la información y la comunicación, expresión que ya está plenamente asentada en el lenguaje jurídico de nuestro tiempo. Las garantías establecidas se proyectan igualmente sobre las intervenciones que tienen por objeto exclusivo el conocimiento de los datos de tráfico u otros datos asociados a la comunicación que están amparados por el secreto de las comunicaciones. Quedan, en cambio, expresamente excluidos los datos a los que puede acceder el fiscal por su propia autoridad por no estar amparados por dicho secreto. De este modo, la normativa aplicable a la obtención de datos asociados será, en definitiva, la específicamente establecida en la ley procesal penal, superándose así los problemas interpretativos generados por la actual ley 25/2007, que habrá de ser reformada en coherencia con este nuevo planteamiento legislativo. La autorización judicial sólo podrá obtenerse si se cumplen tres requisitos. Por un parte, la investigación ha de referirse a determinadas infracciones. Se combina en este punto la gravedad de la pena prevista (prisión igual o superior a cinco años) con un listado de delitos que, por debajo de este listón punitivo, pueden requerir singularmente la utilización a esta diligencia extraordinaria. También será posible la interceptación en la investigación de delitos cometidos a través de medios informáticos o de cualquier otra tecnología de la información o la comunicación, casos en los que esta diligencia puede resultar insustituible como medio indagatorio. Como segundo requisito, se exige un juicio de pronóstico suficientemente fundado sobre la utilidad de la diligencia para obtener datos relevantes que no resultan accesibles a través de otros medios de investigación menos gravosos. Finalmente, la diligencia solo podrá acordarse si se ha establecido suficientemente la relación entre la línea telefónica objeto de intervención y el hecho delictivo. En este punto se extreman las exigencias de concreción y motivación de la solicitud realizada por el fiscal. Igualmente precisa en todo lo relativo al alcance subjetivo y objetivo de la diligencia habrá de ser la resolución judicial que autorice la interceptación».*

5. CONCLUSIONES

Desde los años 90 el auge de la tecnología y de Internet ha sido imparable. Al tiempo que se popularizaba su uso, surgían también nuevas conductas delictivas susceptibles de comisión a través de estos medios, entre las que destacan las relativas a la distribución de pornografía infantil, los daños informáticos, los atentados contra la propiedad intelectual o contra la intimidad. Es la peculiaridad del medio lo que les dota de una especial estructura que ha obligado a la constante especialización de ciertos tipos delictivos, dificultando la tarea de modificación legislativa. Pese a la imposibilidad de un respuesta jurídica, rápida y eficaz, hay que señalar el esfuerzo realizado en las labores de investigación, creándose unidades especializadas en el Cuerpo Nacional de Policía así como en La Guardia Civil, que fueron creciendo a la vez que se extendía el uso de la tecnología entre la población.

Nuevas tecnologías implican nuevas pruebas y también nuevos problemas, el primero de ellos su terminología, dado que no hay un término universal que defina la prueba obtenida de fuentes informáticas, utilizándose unas veces *evidencia digital*, *prueba tecnológica* o *prueba informática*, por citar algunos ejemplos. Tampoco es tarea fácil dilucidar si se trata de nuevos medios o simplemente nuevas fuentes probatorias. Estos son problemas que trata de resolver la Doctrina, que ofrece una variedad de propuestas.

Sin embargo, las mayores dificultades que plantean estas nuevas pruebas consisten en su aportación al proceso y la posibilidad de vulnerar derechos fundamentales en su obtención, especialmente, los contenidos en el artículo 18 CE.

Pese a que *nadie echaría vino nuevo en odres viejos*, en el ámbito civil, y por aplicación supletoria al resto de jurisdicciones, la forma de aportar al proceso la información obtenida de medios electrónicos e informáticos, es adaptarse a las previsiones del artículo 299 de la LEC, resultando lo más habitual en la práctica, la aportación como prueba documental, a veces acompañada de la prueba pericial oportuna, debido a la volatilidad y las infinitas posibilidades de manipulación y tratamiento de este tipo de pruebas y siempre poniendo especial énfasis en lo relativo a la acreditación de su autenticidad e integridad.

Es sin duda en la investigación policial de delitos donde mayor incidencia tiene la posible vulneración de los derechos fundamentales recogidos en el artículo 18 CE, resultando esencial la configuración que la jurisprudencia va realizando de estos derechos. Los mas afectados, en la práctica, son el secreto de las comunicaciones, la inviolabilidad de domicilio y el derecho a la intimidad, que guardan además estrecha relación entre sí, dado que en ocasiones un mismo acto puede vulnerarlos todos.

Las próximas novedades en la materia parece que irán de la mano del Anteproyecto de Ley de Enjuiciamiento Criminal así como de las consecuencias de la reciente Sentencia del TJUE en los asuntos acumulados C-293/12 y C-594/12 (Digital Rights Ireland y Seitlinger y otros), por la que anula la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, por considerar que constituye *«una injerencia de gran magnitud y especial gravedad»* en los derechos fundamentales a la privacidad y a la protección de datos de carácter personal.

Habrá que esperar para ver que consecuencias legislativas y jurisprudenciales tendrán estas modificaciones y los futuros avances tecnológicos que afectarán sin duda a la esfera jurídica; en cualquier caso, *«la tecnología, al igual que los avances científicos, siempre va por delante del Derecho. Pero estos avances sólo deben contextualizarse en el campo de la técnica, ya que al Derecho corresponde una dimensión que excede de los paradójicamente estrechos campos técnicos, los cuales son meros instrumentos materiales»* (STS 143/2013 de 28 de febrero).

6. BIBLIOGRAFÍA

ABEL LLUCH, X. PICÓ I JUNOY, J. RICHARD GONZALEZ, M.(coords.) *"La prueba judicial, desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa"*.La Ley . Madrid, 2011.

FERNÁNDEZ TERUELO, J.G. *"Derecho penal e Internet"*. Lex Nova. Valladolid, 2011

GÓMEZ DE LIAÑO GONZÁLEZ, F. *"El proceso civil"*. Editorial Forum. Oviedo, 2005.

ILLÁN FERNÁNDEZ,J.M. *"Prueba electrónica, eficacia y valoración en el proceso civil"*. Aranzadi, Navarra, 2009.

JAUME BENNASAR, A. *"La validez del documento electrónico y su eficacia en sede procesal"*. Lex Nova. Valladolid, 2010.

MEDRANO I MOLINA,J.M. *"Práctica de la prueba por soportes informáticos y audiovisuales en el proceso penal"*. Universitat de València. (http://aulavirtual.uv.es/)

PASAMAR,A., ORMAZÁBAL SÁNCHEZ,G., BELLIDO ASPAS,M. *"Empresa y prueba informática"*. Bosch, Colección de formación continua Facultad de Derecho de Essade. Barcelona, 2006.

PORTAL MANRUBIA, J. *"La regulación de la prueba electrónica en el proceso penal"*. Revista Aranzadi de Derecho y Proceso Penal, mayo - agosto 2013 , págs. 19 a 41.

VEGAS TORRES, J. *"Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa"*. Cátedra de Investigación Financiera y Forense KPMG-URJC, Universidad Rey Juan Carlos. Madrid, 2011.

VELASCO NUÑEZ, E. (coord.) *"Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia"*. Cuadernos de Derecho Judicial. Consejo General del Poder Judicial, Escuela Judicial. Madrid, 2007.

I CONGRESO CIENTÍFICO DE LA ABOGACÍA DEL PRINCIPADO DE ASTURIAS. *"Libro de ponencias"*. Ilustres Colegios de Abogados de Oviedo y Gijón. Asturias, 2012.