UNIVERSIDAD DE JAÉN

TRABAJO FIN DE MÁSTER

EL VALOR PROBATORIO DE LOS DATOS Y ARCHIVOS MULTIMEDIA EN LOS DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

Miguel Rincón Calahorro
Estudiante Máster Universitario en Derecho Público y de la Administración Pública
Universidad de Jaén

RESÚMEN

En el presente trabajo se analiza las nuevas diligencias de investigación tecnológica introducidas en la Ley de Enjuiciamiento Criminal a través de la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica; con especial dedicación a la novedosa diligencia de análisis y registro de los dispositivos de almacenamiento masivo de información incluida en el Capítulo VIII del Título VIII del Libro II de la norma procesal penal.

ÍNDICE

ABREVIATURAS

Art./Arts.	Artículo/Artículos
ATC	Auto del Tribunal Constitucional
BOE	Boletín Oficial del Estado
CC	Código Civil, de 24 de julio de 1889
CE	Constitución Española, de 29 de diciembre de 1978
CI	Cuestión de Inconstitucionalidad
Coord.	Coordinador
CP	Código Penal, de 23 de noviembre de 1995
FFCCSSEE	Fuerzas y Cuerpos de Seguridad del Estado
FJ	Fundamento Jurídico
ib.	Ibídem
LAJ	Letrado de la Administración de Justicia
LEC	Ley de Enjuiciamiento Civil, de 7 de enero de 2000
LECRIM	Ley de Enjuiciamiento Criminal, de 14 de septiembre de 1882
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial, de 1 de julio de 1985
MP	Magistrado Ponente
Núm.	Número
RA	Recurso de Amparo
Rec.	Recurso
SAP	Sentencia de Audiencia Provincial
Secc.	Sección
STC	Sentencia del Tribunal Consitucional
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y la Comunicación
TS	Tribunal Supremo
op. cit.	Opere citato (Obra citada)
p./p.p.	página/páginas
vid.	véase

Los ordenadores son inútiles. Sólo pueden darte respuestas.

Pablo Picasso

INTRODUCCIÓN

Que duda cabe que, cuando en el seno del Consejo de Ministros del año 1882 se debatió la propuesta de Real Decreto en el que se aprobó la actual Ley de Enjuiciamiento Criminal Manuel Alonso Martínez, el entonces Ministro de Gracia y Justicia no podía imaginar los actuales avances y descubrimientos en el ámbito de la informática y las telecomunicaciones que actualmente presiden nuestro día a día.

Esta realidad tan beneficiosa para la humanidad también ha supuesto que un número ascendente de infracciones penales tienen un componente tecnológico, bien para ampliar su infraestructura y potenciar la consecución de sus fines ilícitos como medio del delito, bien como meros registros y pruebas de la actividad proscrita, como objeto del delito.

En consecuencia, este trabajo tiene como objetivo el análisis y estudio de la reforma de la normativa penal española operada en 2015 en relación con las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución Española y, en concreto, de las diligencias consistentes en el registro de los registros informáticos.

Atendiendo a la peculiaridad de la materia estudiada, que apenas consta de unos años de existencia, se ha realizado un estudio pormenorizado del estado de la cuestión partiendo de la situación precedente a la reforma operada. En lo relativo al análisis de los estudios doctrinales publicados, con la excepción de autorizadas voces doctrinales en la definición de conceptos jurídicos tradicionales clásicos, es importante apuntar que se ha consultado la obra más reciente y vanguardista de los estudiosos del Derecho Procesal Español; lo que ha supuestos que la mayor parte de obras bibliográficas consultadas no excedan de una década de antigüedad.

Misma suerte ha corrido el estudio de la amplísima jurisprudencia existente en el ámbito del Derecho español, en el Derecho Europeo y en el Derecho Internacional; que ha devenido esencial en el resultado de la reforma estudiada y que, como se tendrá ocasión de ver, en no pocos aspectos ha supuestos una mera transposición normativa de doctrinas jurisprudenciales ya consolidadas.

Para la consecución del precitado objetivo, el presente documento se estructura en tres bloques bien diferenciados. En primer lugar se ha procedido a definir los conceptos claves en el ámbito de las nuevas tecnologías y los elementos informáticos claves en marco de las investigaciones penales, tales como la prueba digital o el dispositivo electrónico; así como los mecanismos de garantía de esta nueva fuente probatoria, como son el número IMEI o la función hash.

Asimismo estos nuevos conceptos ya considerados jurídicos se pondrán en relación con la naturaleza y régimen jurídico de prueba tradicional en el ordenamiento español; con especial referencia a la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta reforma, como se tendrá ocasión de comentar, no sólo ha plasmado en un cuerpo legislativo aquellos principios y prevenciones que ya había apuntado la jurisprudencia en materia de prueba digital; sino que viene a incorporar una serie de novedades y diligencias de investigación entre las que se encuentra el registro de dispositivos de almacenamiento masivo de información.

En el segundo bloque se ha considerado imprescindible analizar el haz de derechos fundamentales que una medida de este calado puede tener tanto en el investigado como en su entorno más cercano, pues no debe olvidarse que este tipo de dispositivos en no pocas ocasiones, son utilizadas por personas distintas al investigado.

Para poder dar respuesta a las nuevas formas de delincuencia vinculadas con el uso de nuevas tecnologías, es necesario salvaguardar un delicado equilibrio entre seguridad y privacidad, ponderando la injerencia de la medida estudiada en la esfera de los derechos fundamentales, a fin de no desvirtuar su contenido esencial. Por ello, en este apartado se estudiará la influencia que los datos contenidos en un dispositivo electrónico pueden tener sobre la intimidad, el secreto a las comunicaciones o a la inviolabilidad del domicilio. De igual modo, junto a estos derechos fundamentales consagrados, se analizará también el nuevo derecho a la protección de datos así como la construcción jurisprudencial del nuevo derecho fundamental a la privacidad del entorno virtual, como método de protección del "perfil digital" de la ciudadanía.

En el último bloque se entra de lleno en el contenido de la nueva redacción de la LECRIM, comenzando por la naturaleza de la medida y por el supuesto ordinario de ejecución de la medida en el marco de una entrada y registro domiciliario. Para ello se indicará la necesidad de contar con una habilitación judicial expresa, así como quiénes son los sujetos legitimados para solicitar la medida así como el órgano y los requisitos que se exige para su adopción. A continuación se mostrará también el *íter* procedimental necesario tanto para la correcta ejecución como para la custodia y/o destrucción de la evidencia.

Posteriormente se pasará a estudiar algunos supuestos no ordinarios de adopción de la medida, concretamente aquellos supuestos en los que los CCFFSSEE deben intervenir de manera urgente sin resolución habilitantes; así como aquellos supuestos en los que es el propio investigado el que voluntariamente presta su consentimiento para la ejecución de la diligencia.

I. LA PRUEBA DIGITAL

1. Precisiones terminológicas

El Derecho en general, y la instrucción penal en particular, no pueden permanecer ajenos a los cambios en las realidades humanas,[1] siendo un hecho incontestable que en las últimas décadas se ha producido una auténtica revolución digital en múltiples sectores, entre los que se encuentra la comunicación y la transmisión de informaciones entre sujetos. En el concreto ámbito de la persecución penal, la irrupción progresiva de la informática ha supuesto que ésta pase de ser un mero instrumento de trabajo a un verdadero objeto y medio de prueba, así como un medio de investigación de los delitos.[2]

Sin duda, el primer obstáculo que debemos salvar a los efectos de este trabajo es definir qué entendemos como prueba digital, así como la necesidad de distinguir entre la fuente de prueba, el medio y el soporte de la prueba a los efectos del procedimiento penal,[3] definiendo asimismo algunas de las fuentes de prueba que, debido a su habitualidad, más pronunciamientos judiciales han provocado.

1.1. Prueba digital

Partiendo de la definición de prueba como toda actividad cuya finalidad es acreditar en el proceso la verdad de los hechos expuestos en el procedimiento,[4] SANCHÍS CRESPO (2012) define la prueba digital o electrónica como toda *"información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal",*[5] definición que nos permite deducir cuatro elementos claves de la figura:

---

[1] Amplía esta idea BUENO DE MATA, F. (2015). "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". *Diario La Ley (Núm. 8672),* pp. 1-11.

[2] FISCALÍA GENERAL DEL ESTADO (2019). *Circular 5/2019, sobre registro de dispositivos y equipos informáticos.* p. 2.

[3] De acuerdo con la definición aportada por BANACLOCHE PALAO, J. (2011). "La prueba en el proceso penal". *Aspectos fundamentales del Derecho Procesal Penal.* Madrid. Editorial La Ley (2.ª Edición), p. 273.

[4] DICCIONARIO JURÍDICO BÁSICO (2002). Madrid. Editorial Colex, p. 305.

[5] SANCHÍS CRESPO, C. (2012). "La prueba en soporte electrónico". *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio.* Navarra. Editorial Thomson Reuters Aranzadi (1ª Edición), p. 713.

- Se refiere a cualquier clase de información o dato informático[6] que existe en formato electrónico o digital y que puede afectar a la prueba de las circunstancias determinantes de la responsabilidad penal, como pueden ser documentos, archivos de audio, fotografías o imágenes digitales, videos, email, logs de chats, metadatos, datos de sistema.
- Ha de ser producida, almacenada o transmitida por dispositivos electrónicos físicos,[7] englobando esta categoría no solo a los equipos informáticos tradicionales, sino también los teléfonos móviles o tabletas, así como instrumentos de almacenamiento de datos como DVD o dispositivos USB, tabletas, entre otros supuestos; así como los denominados repositorios remotos o *cloud computing*.
- Ha de tener efectos para acreditar hechos en un proceso abierto en cualquier orden jurisdiccional.
- Debido a la volatilidad y a la facilidad de modificación o alteración de los datos, resulta necesario utilizar técnicas que permitan obtener dichos datos y garantizar que su autenticidad e integridad durante la tramitación del proceso (cadena de custodia).

Sobre esta definición de prueba digital, DELGADO MARTÍN distingue **dos modalidades básicas de prueba electrónica**: los datos e informaciones almacenados en un dispositivo electrónico (ordenadores, discos duros, memorias USB, teléfonos móviles, servidores externos, etc.) y aquéllos transmitidos por cualquier red de comunicación, sea abierta o restringida (Internet, telefonía móvil, etc.).[8] Esta clasificación es fundamental, pues tal y como señala BORGES BLÁZQUEZ, la mayoría de la doctrina ha centrado erróneamente los estudios sobre prueba digital en la figura del documento electrónico, a pesar que no es sino una de las distintas modalidades de prueba electrónica que podemos encontrar,[9] mereciendo también el análisis de otros medios de prueba esencial en el actual espacio cibernético:

---

[6] Entendido el dato informático en el sentido amplio que ofrece el Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001, que define datos informáticos de la siguiente forma: *"se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función"*. Instrumento de Ratificación por España. *Boletín Oficial del Estado, de 17 de septiembre de 2010 (Núm. 226)*, p.p. 78847 a 78896.

[7] Entendido el medio electrónico como aquel definido en el Anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, como *"mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras"*.

[8] DELGADO MARTÍN, J (2017). "La prueba digital. Concepto, clases, aportación al proceso y valoración". *Diario La Ley, Sección Ciberderecho (Núm. 6).*

[9] BORGES BLÁZQUEZ (2018). "La prueba electrónica en el proceso penal y el valor probatorio de las conversaciones mantenidas utilizando programas de mensajería instantánea". *Revista Boliviana de Derecho (Núm. 25)*, p. 543.

a) Correo electrónico

Posiblemente el método más antiguo y extendido de comunicación telemática entre personas[10], se encuentra definido en el artículo 2 h) de la Directiva 2002/58, del Parlamento Europeo y Consejo,[11] 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",* lo que permite que su acreditación pueda hacerse mediante cualquiera de los dispositivos electrónicos de remisión o recepción, y/o en cualquiera de los servidores implicados. Se descompone en dos partes:[12] el mensaje, con sus anexos (texto, audio, video, fotos, etc.) y los metadatos de tráfico, que son los que indican el origen, destino, fecha, hora, duración, tipo y equipo y localización de la comunicación, y que suelen estar en las cabeceras del correo.

Estando de acuerdo con FUENTES SORIANO, esta amplia difusión del correo electrónico como método de comunicación ha supuesto que *"pueda ser el objeto mismo el delito, puede ser exclusivamente la fuente probatoria de la comisión de un delito o puede ser, además del objeto mismo del delito, la prueba de dicho delito"*[13] de manera que es habitual ver en la práctica judicial española el uso del correo electrónico (ya sea mediante su aportación en formato digital o en soporte papel) como fuente de prueba en diversos órdenes jurisdiccionales.

Por último merece la pena recordar que, independientemente del valor probatorio que le sea otorgado por el órgano juzgador, dicha fuente de prueba sólo debe desplegar sus efectos si, como ya se ha apuntado, es posible garantizar su autenticidad e integridad durante la tramitación del proceso.

b) SMS y MMS de los teléfonos móviles

Consiste en un sistema de mensajería que permite enviar y recibir mensajes de texto, en el caso de los SMS (*Short Message Service,* o Servicio de Mensajes Cortos), e incluso acompañado de imágenes, sonido o vídeos y similares en el caso de los MMS (*Multimedia Message Service,* o

---

[10] PUJOL CAPILLA, P. (2014). *La nueva prueba documental en la era digital. Su valoración en juicio*. Madrid. Editorial Jurídica Sepín (1ª Edición), pp. 9-11.

[11] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. *Diario Oficial de las Comunidades Europeas, de 31 de julio de 2002 (Núm. 201)*, p.p. 37 a 47.

[12] Según el art. 3 de la Ley 25/2007, de 18 de octubre, de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *Boletín Oficial del Estado, de 19 de octubre de 2007 (Núm. 251)* p.p. 42517-42523.

[13] FUENTES SORIANO, O. (2017). "El valor probatorio de los correos electrónicos", en ASENCIO MELLADO J.M. (Coord.) *El proceso penal ante nuevas formas de delincuencia.* Valencia. Editorial Tirant lo Blanch (1ª Edición), p. 4.

Servicio de Mensajes Multimedia), que permite a los teléfonos móviles utilizar este tipo de comunicación; por lo que tienen un tratamiento muy similar al del correo electrónico.

Aunque actualmente está disminuyendo su uso, siguen estando presentes como elemento de prueba fundamental en el proceso penal para acreditar la comisión de determinados tipos penales, como el caso de las injurias, las amenazas, el acoso o determinados delitos contra la intimidad.

c) La agenda de contactos de los teléfonos móviles

Consistente en el almacenamiento digital de los nombres, teléfonos u otros datos de contacto en la tarjeta o el almacenamiento del terminal móvil, dado el carácter esencial que han tenido en la persecución de determinados delitos de salud pública o terrorismo, ha dado lugar a una prolija doctrina tanto del Tribunal Constitucional como del Tribunal Supremo, que se analizará más adelante.

d) El Número IMEI y del IMSI de un teléfono

El IMEI o Identidad Internacional del Equipo Móvil corresponde con el número de serie del equipo móvil, pudiendo conocerse mediante el tecleo del código "asterisco, almohadilla, 06, almohadilla", sin que para ello sea necesario, ni por ello implique, el acceso a ningún dato de la memoria de dicho equipo. Este número de serie resulta esencial para, entre otras medidas, la solicitud de orden de identificación para el operador de la correspondiente intervención de las conversaciones.

Por otro lado el IMSI o International Mobile Suscriber Identity (Identidad Internacional del Abonado a un Móvil) es un código de identificación único para cada dispositivo móvil, integrado en la tarjeta chip SIM (Subscriber Identy Module) que se inserta en el teléfono móvil para asignarle el número de abonado o MSISDN (Mobile Station Integrated Services Digital Network), que permite su identificación y proporciona una medida adicional de seguridad en la telefonía móvil y, sobre todo, facilita la prevención del fraude en la telefonía celular.

En ambos casos la correcta identificación de estos terminales resulta clave en la investigación penal: imaginemos que el rastreo de una determinada llamada telefónica nos lleva hacia un número IMEI que, previa identificación por las FFCCSSEE deviene en una orden de entrada y registro en domicilio. Si se deseara analizar el contenido de dicho terminal, resultará imprescindible que el órgano judicial habilitante incorpore explícitamente cómo se ha llegado a la conclusión de que dicho terminal resulta relevante para la instrucción; so pena de incurrir en ilegalidad en el modo de obtención de la prueba.

e) WhatsApp y otros sistemas de mensajería instantánea

Consisten en aplicaciones de mensajería instantánea que permite el envío de mensajes de texto, imágenes, sonido, vídeos con los números de teléfonos que se encuentren en los dispositivos o las cuentas de usuario contenidas en la aplicación. La principal diferencia que plantean respecto al correo electrónico o al SMS es que la información transmitida no se conserva en un servidor externo, impidiendo que la autoridad judicial pueda solicitar a la empresa prestadora del servicio que certifique que el contenido de mensajes enviados o recibidos, teniendo que acudirse a los dispositivos electrónicos usados para su conversación.

Su uso como medio de prueba se ha puesto en práctica a través de una amplia casuística,[14] así como amparada por el Tribunal Supremo a partir de su Auto Núm. 392/2013, de 14 de febrero, en el que se amparaba una orden judicial que preveía la intervención y registro de las comunicaciones vía Whatsapp obrantes los terminales móviles de los imputados.[15]

f) Redes sociales, foros, chats, blogs,…

Ampliamente populares son espacios como Facebook, Twitter, Youtube, Instangram, etc., encontrándonos ante verdaderas comunidades o lugares virtuales que se utilizan para introducir las ideas, pensamientos, hobbies o similares en los cuales se pueden intercambiar opiniones, experiencias o pensamientos sobre distintos temas. A su vez, nos permite comunicarnos con personas de diferentes partes del mundo en tiempo real.

Al contrario que en el caso anterior, la nota técnica característica es que la información transmitida generalmente se conserva en un servidor externo (o servidores), lo cual permitirá como parte de medidas encaminadas a la averiguación de determinados delitos, el libramos de oficios a las empresas tenedoras de dichos datos; así como el acceso remoto a los datos contenidas en ellas, generalmente a través de un usuario y una contraseña; no siendo necesario disponer del terminal desde el que se generó la prueba digital.

Por ejemplo, resulta posible acceder a una conversación realizada por Facebook desde un ordenador a través del acceso a la misma cuenta en la red social desde un terminal móvil. Ello supone, como se analizará más adelante, que la orden habilitante para el registro del dispositivo

---

[14] *Vid.* entre otras las SAP Cádiz (Secc. 3ª) Núm. 31/2014, de 28 de enero (ECLI: ES:APCA:2014:122), respecto a la prueba de un delito de lesiones; SAP Pontevedra (Secc. 4ª) Núm. 10/2014, de 10 de enero (ECLI: ES:APPO:2014:18), como justificante del carácter vejatorio y ofensivo de las manifestaciones de la denunciante; o la SAP Madrid (Secc. 27ª) Núm. 12/2013, de 5 de abril, (ECLI: ES:APM:2013:5798) como acreditación de un delito contra la mujer.

[15] *Vid.* ATS (Sala 2ª) Núm. 392/2013, de 14 de febrero (ECLI: ES:TS:2013:1800A).

electrónico que contenga la información relevante para la instrucción deberá contener una previsión explícita sobre el acceso y registro a las redes sociales que se encuentran abiertas (sin necesidad de incluir contraseña) en el terminal o bien que se disponga de dicha contraseña.

1.2. Dispositivo electrónico

Analizadas algunas de las manifestaciones más comunes de la prueba digital que podemos encontrar, es ineludible continuar con la definición de los soportes o instrumentos que sirven para contener estas fuentes, los cuales denominaremos **dispositivos de almacenamiento masivo de información.**

La nueva regulación de la LECRIM que más adelante se analizará utiliza el concepto de "dispositivos de almacenamiento masivo de información", como aquellos dispositivos electrónicos que utilizan un *"lenguaje binario a través de un sistema que trasforma impulsos o estímulos eléctricos o fotosensibles y, por cuya descomposición y recomposición informática grabada en un formato electrónico, genera y almacena la información"*.[16] Dicho lenguaje, ininteligible para cualquier profano en la materia, se visualiza en modo de texto o imagen en una pantalla a través de una traducción (descodificación) en un lenguaje alfabético común. Partiendo de la regulación contenida en el artículo 588 sexies a. 1) de la LECRIM que más adelante se analizará, podemos agrupar los dispositivos de almacenamiento masivo de información en cuatro grandes categorías:[17]

a) Dispositivos magnéticos, entendidas estas como las unidades de disco duro que componen los ordenadores, entendidos como dispositivos que permiten el tratamiento automatizado de datos en ejecución de un programa o software.[18]

b) Instrumentos de comunicación telefónica o telemática, como dispositivos cuya función primordial es la transmisión de datos (comunicación telemática) y/o de la voz (comunicación telefónica), como es el caso de los terminales móviles, tablets, dispositivos de navegación, etc.

---

[16] GARCÍA TORRES M.L. (2011). "La tramitación electrónica de los procedimientos judiciales, según ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil". *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Núm. 3).*

[17] La Fiscalía General del Estado en su Circular 5/2019, *op. cit.,* ha realizado esta agrupación únicamente sobre tres grandes grupos: dispositivos magnéticos (fundamentalmente, unidades de disco duro o HDD, del inglés Hard Disk Drive), dispositivos ópticos (CD, DVD o BD) y los dispositivos de memoria sólida o SSD (acrónimo inglés de solid-state drive) (tarjetas de memoria, memorias USB, etc.); añadiendo en último lugar de manera desorganizada el resto de dispositivos que se mencionan, por lo que se considera que dicha agrupación no presenta el adecuado rigorismo académico.

[18] De acuerdo con el tenor literal del art. 19 del Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001, *op. cit.*

c) Dispositivos cuya función primordial es el almacenamiento masivo de información digital (computer data), como es el caso de los discos duros (portátiles o no), los CDs y DVD, dos dispositivos USB o SD o cualquier dispositivo análogo.

d) Repositorios telemático de datos, entendidos estos como sitios donde se almacena o deposita la información en formato digital (datos) y al que se accede a través de una red de comunicación; coloquialmente conocidos como sistemas de almacenamiento en la nube o *cloud computing*. Son cada vez más frecuentes los supuestos en los que las empresas (información de su objeto de negocio) y los particulares (documentos, fotos, videos, contactos….) almacenan sus datos, de forma temporal o definitivamente, en servidores en la nube.[19]

Como se analizará posteriormente, debido a la diversa naturaleza de los datos resulta razonable que nuestro ordenamiento jurídico haya realizado un tratamiento procesal unitario a los datos contenidos en los distintos dispositivos de almacenamiento, que a su vez son reveladores del perfil personal del investigado, configurando todo un derecho constitucional de nueva generación: la protección del propio entorno virtual.

1.3. Entorno digital

Fruto de la constante incorporación de tecnologías a nuestro día a día, las personas hemos ido realizando cada vez más actividades empleando estas TIC´s en múltiples ámbitos (laboral, familiar, social, económico, académico, etc…) que no hace sino generar un *"rastro o huella digital"* que, en ocasiones ha resultado imprescindible en la investigación por parte de los poderes públicos de actuaciones ilícitas. De esta manera autores como GONZÁLEZ-CUÉLLAR SERRANO definen el entorno digital o virtual como aquel *"conjunto de informaciones en formato digital que una persona genera con su actividad mediante dispositivos electrónicos, de manera consciente o inconsciente, con voluntariedad o sin ella"*.[20] Este concepto, introducido antes de la reforma de 2015, ya fue reconocido en la paradigmática STS Núm. 342/2013, de 17 de abril; poniéndose de manifiesto la existencia un entorno digital susceptible de un determinado nivel de protección frente a la actividad inquisitiva del Estado, so pena de suponer un riesgo de lesividad para los derechos fundamentales de las personas investigadas.[21]

---

[19] COTINO HUESO, L. (2015). "Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa". *Revista catalana de dret públic (Núm. 51)*, pp. 86.

[20] GONZÁLEZ-CUÉLLAR SERRANO, N. (2008). "Garantías constitucionales de la persecución penal en el entorno digital"; en GÓMEZ COLOMER, J. L. (Coord.). *Prueba y proceso penal. Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado.* Valencia. Editorial Tirant lo Blanch (1ª Edición).

[21] FJ Séptimo de la STS (Sala 2ª) Núm. 342/2013, de 17 de abril (ECLI: ES:TS:2013:2222).

La importancia de tal garantía no es otra que la salvaguarda de los datos contenidos en tales dispositivos (gustos, aficiones, opiniones políticas, creencias, datos de geolocalización, etc…) que por sí solos no tendrían una especial relevancia, pero que puestos en conjunto permiten general un "perfil digital" del investigado que pone en tela de juicio derecho fundamentales como la intimidad o el secreto a las comunicaciones.

1.4. Huella digital o código hash

Sin entrar en profundidad en la complejidad técnica que la materia supone, podemos definir los algoritmos hash como *"aquellas funciones matemáticas que se extraen mediante el uso de un software matemático que crea un código de identificación alfanumérico que compartirán la prueba original y su clon, a fin de garantizar la integridad de una prueba informática, de modo que la sola alteración, eliminación de un bit así como la aparición de uno o más bits nuevos arrojarían códigos hash distintos"*.[22] Por ello, para garantizar la cadena de custodia en el caso de copia de dispositivos electrónicos será imprescindible que la cifra numérica arrojada por el soporte original y por la copia sea idéntica, indicando que no se ha producido ningún tipo de alteración y garantizando así la integridad de la prueba digital.

2. Naturaleza jurídica de la prueba digital

Una vez precisados algunos conceptos claves en el presente trabajo, se antoja imprescindible entrar a analizar la naturaleza jurídica de la prueba digital, debiendo preguntarnos si nos encontramos ante una prueba documental especial o si, por el contrario, nos encontramos ante una prueba de reconocimiento judicial que debe ser examinada por el órgano judicial; siendo este aspecto clave para la determinación de sus normas reguladoras y el modo en el que suplirán los vacíos legales que genere.[23]

Para poder dar una respuesta satisfactoria se seguirá el razonamiento planteado por ABEL LLUNCH y PICÓ I JUNOY (2011), los cuales plantean tres posibilidades o teorías de análisis:[24]

---

[22] FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A. (2016). "Registro de dispositivos de almacenamiento masivo de información". *Dereito: revista xurídica da Universidade de Santiago de Compostela. Volumen 25 (Núm. 2)*, p. 41.

[23] En este sentido se pronuncian URBANO CASTRILLO, E. y MAGRO SERVET, V. (2003). *La prueba tecnológica en la Ley de Enjuiciamiento Civil*. Navarra. Editorial Aranzadi, p.p. 39-40.

[24] Extraídas de ABEL LLUNCH, X. y PICÓ I JUNOY, J. (Coord.). (2011). *La prueba electrónica*. Barcelona. Editorial Bosch (1ª Edición), p.p. 107-113.

- La **teoría autónoma,** que sostiene que la prueba electrónica presenta unas características propias y particulares, diferentes con los medios convencionales de prueba, especialmente respecto a la documental.

- La **teoría analógica**, que propugna que los tantos los medios de prueba convencionales como los nuevos medios de prueba surgidos en el ámbito digital son equiparables, en los que únicamente se ha modificado el antiguo soporte papel hacia un nuevo soporte electrónico. No obstante, la diferencia entre ambos medios de prueba estiba en que, mientras la prueba documental tradicional quedaba sometida a las reglas *"de la prueba tasada"*, la nueva prueba digital no puede sino someterse a *"las reglas de la sana crítica"*.

- La **teoría de la equivalencia funcional,** que viene a suponer la no distinción de la naturaleza jurídica de la prueba electrónica frente a la incorporada mediante soportes materiales, pues ambos *"producen efectos jurídicos y tienen la misma fuerza probatoria que los tradicionales*[25]*"*.

Si nos acercamos a nuestra norma procesal civil, de subsidiaria aplicación, el párrafo 13º del apartado XI de la Exposición de Motivos de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en el que se afirma que *"no es de excluir, sino que la ley lo prevé, la utilización de nuevos instrumentos probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales"*.

A mayor abundamiento, tanto el artículo 3.8 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, al afirmar que *"el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio";* como el artículo 24.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, cuando determina que *"en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental";* vienen a apoyar esta equiparación de la prueba electrónica con la tradicional prueba documental.

---

[25] ILLÁN FERNÁNDEZ, J.M. (2009). *La prueba electrónica, eficacia y valoración en el proceso civil.* Navarra. Editorial Aranzadi (1ª Edición), p. 254.

Dicha predisposición legislativa hacia la equiparación absoluta parece tener cabida también a nivel jurisprudencial, como así lo han ratificado los Tribunales Superiores de Justicia de Madrid[26] y de Andalucía[27] al afirmar ambos que *"el concepto de documento no puede interpretarse de una forma tan restrictiva que solo abarque representaciones escritas, muy al contrario, hay que considerar como tal todo objeto que cumpla la función de dar a conocer determinados elementos en el representados, bien por escrito, imágenes o sonidos."*

3. Régimen jurídico de la prueba digital

3.1. La deficiente y dispersa regulación previa a 2015

Uno de los problemas a los que tradicionalmente se han enfrentado los operadores jurídicos ha sido la necesidad de dilucidar como la prueba digital accede al proceso. Ello se debe no sólo a razones de logística procesal, sino por razones puramente de práctica jurídica, ya que en muchos casos los tribunales son reacios a que se aporten los soportes informáticos, y tienden más a que el propio contenido de la prueba electrónica se aporte mediante los medios de prueba tradicionales, fundamentalmente en papel.

Ahora bien, si partimos del derecho de todo ciudadano a utilizar todos los medios de prueba pertinentes para poder defenderse sin limitación alguna recogido en el artículo 24.2 CE,[28] debemos afirmar que aun hoy no existe un cuerpo normativo específico y concreto dedicado a regular la prueba digital en el ámbito penal, debiendo aplicar supletoriamente lo dispuesto para el proceso civil. Por ello, la primera parada en nuestro camino ha de ser la agrupación que nos ofrece el artículo 299 de la Ley de Enjuiciamiento Civil[29], en la que podemos diferenciar:

---

[26] FJ Primero de la STSJ Madrid (Sala de lo Social) Núm 696/2004, de 6 de julio (ECLI: ES:TSJM: 2004:9328).

[27] STSJ Andalucía (Sala de lo Social) Núm. 145/2000, de 28 de enero (ECLI: ES:TSJAND:2000:1430).

[28] Aclarado no obstante en la doctrina constitucional en innumerables sentencias, que éste *"no comprende un hipotético derecho a una actividad probatoria ilimitada, atendiendo a la naturaleza del derecho como de configuración legal, por lo que su ejercicio habrá de acomodarse a las exigencias del proceso y a las normas legales que lo prevean, cuya interpretación en relación a la admisión de los medios de prueba corresponde a los Tribunales ordinarios en ejercicio de sus funciones jurisdiccionales"* tal y como se desprende del ATC (Secc. 4ª) Núm. 219/1999, de 17 septiembre (ECLI: ES:TC:1999:219A).

[29] ORTOÑO ARTÉS, C. (2001). *El avance tecnológico y los nuevos medios de prueba en la LEC. Régimen jurídico de Internet.* Madrid. Editorial La Ley (1ª Edición), p.p. 489-512.

a) Los documentos probatorios entendidos en sentido clásicos definidos en el artículo 299.1 LEC: el interrogatorio de las partes, los documentos públicos y privados, el dictamen de peritos, reconocimiento judicial y el interrogatorio de testigos; que no obstante podrán tener el carácter de digital si lo ponemos en relación con el artículo 3.5 de la Ley 59/2003 de firma electrónica, que 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",* pudiendo tener éste el carácter de público o privado.

b) Los medios probatorios modernos o actuales, entendidos en la redacción que le dio el legislador del año 2000 y definidos en el apartado segundo, que comprenderá los audiovisuales y los instrumentos informáticos.

c) Los medios probatorios futuros o que están por llegar, previstos en el apartado tercero, dejando al arbitrio del juez determinar como prueba alguna fuente no predeterminada, que pueda manifestarse en el futuro.

Junto a esta regulación básica de los medios de prueba, también podemos encontrar otros ejemplos relativos a la prueba dispersos en otros cuerpos procesales, como el caso del artículo 230 LOPJ, que obliga a Juzgados, Tribunales y Fiscalías a utilizar medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad, y por lo tanto, también para poder analizar las fuentes de prueba electrónicas aportadas por las partes que requieran de los mismos;[30] o el artículo 26 del Código Penal que permite la aportación de prueba en formatos distintos al tradicional papel.[31] Todo lo anterior no hace sino dotar de sentido la voluntad del legislador del año 2000, quien en la propia Exposición de Motivos de la Ley de Enjuiciamiento Civil ya abría la puerta al valor probatorio de nuevos medios que tecnológicamente se desarrollarían con posterioridad, al exponer:

"Podrán confeccionarse y aportarse (...) y no es de excluir, sino que la ley lo prevé, la utilización de nuevos instrumentos probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas con los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales."[32]

---

[30] Artículo 230.1 LOPJ: *"Los juzgados y tribunales y las fiscalías están obligados a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establecen el capítulo I bis de este título y la normativa orgánica de protección de datos personales."*

[31] 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."*

[32] Párrafo 13º del Fundamento XI de la Exposición de Motivos de la Ley de Enjuiciamiento Civil.

Este *"numerus apertus"* de medios de prueba conlleva que salvo contadas ocasiones como en la reforma de la LECRIM operada en 2015, en las que por vía legislativa se ha procedido a recoger instrumentos específicos de prueba; la realidad de la prueba digital se ha venido incorporado a nuestro ordenamiento jurídico a través de un consolidado cuerpo de doctrina constitucional e internacional que ha adaptado las bases decimonónicas de nuestra normativa procesal a las exigencias y requisitos esenciales para el adecuado tratamiento de la prueba digital en la instrucción penal;[33] destacándose siempre la reserva de Ley como garantía de la seguridad jurídica en el ámbito de los derechos fundamentales.

Ya el Tribunal Supremo en su Sentencia 1335/2001, de 19 de julio, vino a reconocer que el artículo 579 de la entonces vigente LECRIM era insuficiente para "*sustentar las investigaciones a través de medios tecnológicos*", concretamente la ausencia de una previsión sobre los supuestos que justifican la intervención de los dispositivos de almacenamiento de información.[34] Primera llamada de atención que posteriormente fue secundada por el Tribunal Constitucional en su STC Núm. 184/2003, de 23 de octubre, la cual reiteró la falta de previsión normativa sobre el plazo máximo de la duración de las intervenciones.[35]

En la misma y en el plano internacional, el Tribunal Europeo de Derecho Humanos también ha tenido posibilidad de pronunciarse en sus STEDH Caso Prado Burgallo contra España, de 18 de febrero de 2003;[36] la STEDH Caso Valenzuela Contreras contra España, de 30 de julio de 1988;[37] y la STEDH Caso Abdulkadir Coban contra España, de 26 de septiembre de 2006.[38] En esta última sentencia, el Tribunal Europeo de Derechos Humanos incluso sugirió que era deseable *"una modificación legislativa que incorporase a la Ley los principios que se desprenden de la jurisprudencia del Tribunal"*, reiterando además que en el Derecho español existía ya una jurisprudencia consolidada y bien establecida en la materia.

---

[33] En este sentido autoras como ARMENTA DEU, T. (2018). "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, Whatsapp, redes sociales): entre la insuficiencia y la incertidumbre". *Revista de Internet, Derecho y Política (Núm. 27)*, p. 70; o LÓPEZ-BARAJAS PEREA, I. (2017). "Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley". *Revista de Derecho Político (Núm. 98)*, p. 97.

[34] FJ Decimonoveno de la STS (Sala 2ª) Núm. 1335/2001, de 19 de julio (ECLI: ES:TS:2001:6389).

[35] FJ Sexto de la STC (Pleno) Núm. 184/2003, de 23 de octubre (ECLI: ES:TC:2003:184).

[36] ECLI: CE:ECHR:2011:1018DEC002121809.

[37] ECLI: CE:ECHR:1998:0730JUD002767195.

[38] ECLI: CE:ECHR:2006:0925DEC001706002.

No obstante, es unánime la doctrina al afirmar que el punto de inflexión en la materia nos lo ofreció el Tribunal Constitucional a través de su STC Núm. 145/2014, de 22 de septiembre, al atacar frontalmente la regulación contenida en el pretérito artículo 579 LECRIM por considerar que era insuficiente para la persecución y esclarecimiento de los delitos vinculados a las Tecnologías de la Comunicación y la Información, estimando parcialmente un recurso de amparo por ausencia de garantías constitucionales en unas escuchas obtenidas en unos calabozos mediante dispositivos de grabación, a pesar de su autorización judicial, por no existir habilitación legal para ello.[39] En su análisis, el intérprete constitucional reitera su posición de que no toda injerencia en las comunicaciones puede quedar amparada con la autorización judicial, sino que debe existir además una expresa habilitación legal que lo prevea, al menos en lo que a un contenido mínimo supone, en aras de proteger al ciudadano ante actuaciones arbitrarias del Estado.[40]

---

[39] Fundamento Jurídico 7 de la STC (Sala 2ª) Núm. 145/2014, de 22 de septiembre (ECLI:ES:TC:2014:145), en el que se declara que *"es doctrina constante de este Tribunal (por todas, STC 49/1999, de 5 de abril, FJ 3) que aunque la literalidad de dicho precepto («se garantiza el secreto de las comunicaciones y, en especial, las postales, telegráficas y telefónicas, salvo resolución judicial») puede inducir a pensar que la única garantía que establece inmediatamente la Constitución es la exigencia de autorización judicial, un análisis más detenido de la cuestión pone de manifiesto lo contrario, ya que, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, además, una habilitación legal. Esa misma jurisprudencia dispone que la reserva de ley constituye «el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas», lo que «implica exigencias respecto del contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate», pero que en todo caso determinan que «el legislador ha de hacer el 'máximo esfuerzo posible' para garantizar la seguridad jurídica», esto es, «la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho» (STC 49/1999, FJ 4). Profundizando en esa exigencia, en la STC 169/2001, 16 de julio, FJ 6, sostuvimos, con abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, en cuanto a las características exigidas por la seguridad jurídica respecto de la calidad de la ley habilitadora de las injerencias, que «la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad."*

[40] Así se recuerda que la STC (Sala 2ª) Núm. 169/2001, 16 de julio (ECLI:ES:TC:2001:169), sostuvo, con abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, en cuanto a las características exigidas por la seguridad jurídica respecto de la calidad de la ley habilitadora de las injerencias, que "*la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad. Esa reserva de ley a la que, con carácter general, somete la Constitución la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, también el del art. 18.3 CE, desempeña una doble función; a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos "únicamente al imperio de la Ley" y no existe, en puridad, la vinculación al precedente, constituye, adicionalmente, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas."*

3.2. Los intentos de reformas integrales de la LECRIM.

Al hilo de las llamadas de atención que ya habían efectuado los distintos tribunales, era evidente la necesidad de implantar una nueva Ley de Enjuiciamiento Criminal.[41] Para dar respuesta a esta demanda surgieron tanto el Anteproyecto de Ley para un nuevo proceso penal, elaborado en 2011 por la Secretaría General Técnica del Ministerio de Justicia; como el Borrador de Código Procesal Penal, elaborado por la Comisión Institucional para la elaboración de un texto articulado de la Ley de Enjuiciamiento Criminal constituida *ad hoc* por Acuerdo del Consejo de Ministros de 2 de marzo de 2012.

Lamentablemente, y bajo la excusa de falta de consenso parlamentario para ello, ambos proyectos resultaron malogrados, y el legislador prefirió realizar una reforma parcial de la vetusta LECRIM de 1882 por medio de dos cuerpos legislativos: el primero, plasmado en la Ley Orgánica 13/2015, de 5 de octubre, que centrará el resto del presente trabajo, destinada a recoger aquellas materias de carácter orgánico por afectar a derechos fundamentales, como el estatuto del investigado y la regulación de las nuevas medidas tecnológicas; mientras que el segundo, operado por la Ley 41/2015, de 5 de octubre, se ha reservado para materias ordinarias; entre las que se encuentran las medias de agilización de la justicia penal, la regulación de la generalización de la segunda instancia, así como los procesos monitorio penal, de decomiso autónomo o la ampliación del recurso de revisión.

3.3. La reforma operada por la LO 13/2015, de 5 de octubre.

La repuesta que se da desde el poder legislativo a la exigencia de actualización de las medidas de investigación penal a los nuevos escenarios tecnológicos la encontramos en la Ley Orgánica 13/2015, de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica; en cuyo preámbulo se alude expresamente a la ya comentada STC Núm. 145/2014, de 22 de septiembre, al afirmar el apartado IV que:

> *"(...) Recientemente, el Tribunal Constitucional ha apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. Hoy por hoy, carecen de cobertura y su subsanación no puede obtenerse acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable. Solo así se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal."*

[41] Entre otros, BUENO DE MATA (2015). *op. cit.,* p.1-2 o LÓPEZ-BARAJAS PEREA. (2017). LÓPEZ-BARAJAS PEREA, I. (2017). "Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley". Revista de Derecho Político (Núm. 98), p. 98.

De este modo nos encontramos pues ante una modificación parcial de la ley procesal penal que viene a paliar la insuficiente regulación de la que adolecían la mayoría de las medidas de investigación tecnológica, mediante la configuración de un nuevo Título VIII del Libro II renombrado "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución".

Con una mejorable ordenación sistemática,[42] dicho Título incluirá en sus tres primeros capítulos las ya tradicionales medidas de investigación consistentes en la entrada y registro de lugares cerrados (Capítulo I), el registro de libros y papeles (Capítulo II) y la interceptación de correspondencia escrita y telegráfica (Capítulo III), aunque con una nueva disposición al hallazgo casual de nuevos delitos. Sobre estos preceptos ya existentes en nuestra ley procesal, la nueva redacción de 2015 va a añadir unos principios rectores que ya venían recogidos en la jurisprudencia recaída en los últimos años en torno a los presupuestos que deben concurrir para toda medida limitativa de un derecho fundamental,[43] que se incluirán junto con las disposiciones comunes a las nuevas medidas de investigación tecnológica en un nuevo Capítulo IV; desarrollándose cada una de ellas en los sucesivos capítulos: interceptación de las comunicaciones telefónicas y telemáticas (Capítulo V); la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (Capítulo VI); la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen (Capítulo VIII); el registro de dispositivos de almacenamiento masivo de información (Capítulo VIII); y los registros remotos sobre equipos informáticos (Capítulo IX).

---

[42] LÓPEZ-BARAJAS PEREA. (2017). *ib. p. 99;* al afirmar que "A*unque con un criticable criterio de ordenación sistemática,(...)".*

[43] Dicha enumeración de requisitos generales para todas las medidas es criticada por OTAMENDI ZOZAYA, F. (2017). *Las últimas reformas de la Ley de Enjuiciamiento Criminal*. Editorial Dykinson (1ª Edición), p. 104;se al indicar que la nueva redacción de la LECRIM *"introduce una serie de requisitos que son de difícil aplicación a la totalidad de esas medidas de investigación tecnológica que se mencionan en el nombre del capítulo y sólo pueden ser comprendidas si se refieren a las medidas de intervención telefónica. Así, por ejemplo, la necesidad de dar, siempre y en todo caso, traslado al Ministerio Fiscal para que informe, en el plazo de 24 horas, sobre la adopción de todas estas medidas no parece que tenga ningún sentido, por ejemplo para solicitar la titularidad de una dirección IP o para solicitar los datos de tráfico de llamadas. No entendiéndose tampoco la imposición de un plazo tan breve, que si bien puede tener sentido cuando de la intervención de las comunicaciones telefónicas se trata, pues por regla general dicha intervención conviene hacerla a la mayor brevedad a fin de no perder información que puede ser preciosa para la investigación, no parece que sea necesario cuando se refiere a otro tipo de medidas de investigación tecnológica en las que la información que se va a recabar se conserva durante muchos meses y, lo que es menos comprensible, se tarda en entregar por parte de las operadoras, en muchas ocasiones, semanas enteras desde que se recibe la solicitud y ello a pesar de que, conforme a la ley 25/2007, la información deberá entregarse en el plazo de 72 horas, salvo que se dispusiera lo contrario en la resolución judicial que acuerda recabar dicha información. Es decir, el legislador impone plazos brevísimos al Ministerio Fiscal y al juez para resolver sobre la petición policial, pero después la recepción de la información que se recaba puede tardar incluso meses, en función de la diligencia que adopte el destinatario de la medida, lo que no tiene ningún sentido."*

Sin duda son estos principios rectores, recogidos en el artículo 588 bis a), los que vienen a recoger la gran labor consagrada de la literatura constitucional,[44] que han de ser de aplicación a todas las diligencias de investigación tecnológica para garantizar la no conculcación de los derechos fundamentales:

a) **Principio de especialidad**

De acuerdo con este principio, se exige que la medida acordada esté relacionada con un hecho concreto, determinado y definido, sin que quepa la validez de medidas de investigación tecnológica que busquen prevenir o descubrir delitos o despejar sospechas sin base objetiva, mediante la instrucción de las llamadas "investigaciones prosprectivas" o causas generalistas.

Este principio de especialidad. ya estaba firmemente asentado en la jurisprudencia del Tribunal Supremo anterior a la reforma de 2015, cuando afirma que:

> *(...) cuando se trata de investigaciones realizadas mediante intervenciones telefónicas, entre los requisitos que deben ser observados se encuentra el de la especialidad de la medida, en el sentido de que la intervención debe de estar orientada hacia la investigación de un delito concreto, sin que sean lícitas las observaciones encaminadas a una prospección sobre la conducta de una persona en general. Lo que no excluye que los hallazgos casuales sugerentes de la posible comisión de otros delitos distintos no sean válidos, sino que la continuidad en la investigación de ese hecho delictivo nuevo requiere de una renovada autorización judicial.*[45]

Interpretación confirmada también por el máximo intérprete constitucional al afirmar que es necesario que la medida busque investigar un hecho que integre el objeto del proceso penal, y no meros indicios o sospechas, pues *"un acto instructorio que limite un derecho fundamental no puede estar dirigido exclusivamente a obtener meros indicios o sospechas de criminalidad, sino debe tener como finalidad la preconstitución de la prueba de los hechos que integran el objeto del proceso penal."*[46]

---

[44] Entre otras la STC (Pleno) Núm. 222/2012, de 27 de noviembre (ECLI: ES:TC:2012:222); la STC (Pleno) Núm. 12/2008, de 29 de enero (ECLI: ES:TC:2008:12); o la STC (Sala 1ª) Núm. 253/2006, de 11 de septiembre (ECLI: ES:TC:2006:253).

[45] Opinión ya contenida, entre otras en la STS (Sala 2ª) Núm. 991/2016, de 12 de enero (ECLI: ES:TS: 2017:47); la STS (Sala 2ª) Núm. 717/2016, de 27 de septiembre (ECLI: ES:TS:2016:4173); la STS (Sala 2ª) Núm. 656/2015, de 10 de noviembre (ECLI: ES:TS:2015:4803); la STS (Sala 2ª) Núm. 689/2014, de 21 de octubre (ECLI: ES:TS:2014:4829); o la STS (Sala 2ª) Núm. 1046/2013, de 22 de julio (ECLI: ES:TS: 2013:4300).

[46] Entre otras, STC (Sala 2ª) Núm. 26/2006, de 30 de enero (ECLI: ES:TC:2006:26); STC (Sala 2ª) Núm. 165/2005, de 20 de junio (ECLI: ES:TC:2005:165); y STC (Sala 1ª) Núm. 207/1996, de 22 de enero (ECLI: ES:TC:1996:207).

No obstante, y como con posterioridad en este trabajo se desarrollará, se contempla la posibilidad que las medidas acordadas por la autoridad en el procedimiento de investigación de un delito puedan dar lugar al llamado *"descubrimiento casual"* de otro delito; así como el hecho que las pruebas obtenidas por la diligencia de investigación puedan ser puesta a disposición por su relevancia para la instrucción de otra causa distinta, de acuerdo con lo dispuesto en el artículo 588 bis i) y con la propia jurisprudencia constitucional, extremo ya admitido desde la STC 41/1998, de 24 de febrero, al afirmar que:

> *(...) la Constitución no exige, en modo alguno, que el funcionario que se encuentra investigando unos hechos de apariencia delictiva cierre los ojos ante los indicios de delito que se presentaren a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en su investigación oficial, siempre que ésta no sea utilizada fraudulentamente para burlar las garantías de los derechos fundamentales.*[47]

b) **<u>Principio de idoneidad</u>**

Exigencia para el intructor de adoptar la medida más adecuada y útil al hecho que se pretende investigar, tanto en lo relativo al objeto de la instrucción, como al ámbito subjetivo y temporal. En palabras del TS, la cuestión de idoneidad *"no depende de la concreción del peligro, sino exclusivamente de la abstracta adecuación al mismo que ha establecido el legislador."*[48] Sobre a la *extensión objetiva,* la aplicación del principio de idoneidad exige limitar las medidas de investigación al contenido concreto de la autorización (por ejemplo, al dispositivo electrónico singularmente identificado en la autorización judicial y cuyo contenido previsiblemente pueda ser relevante al objeto de la investigación. En lo que respecta a la *extensión subjetiva,* resulta imprescindible considerar que las medidas adoptadas pueden afectar a terceras personas distintas del investigado, por lo que sólo deben adoptarse cuando sea necesario para los fines de la investigación *ex* artículo 588 bis h).

Finalmente, en lo relativo a la *extensión temporal* se considera que el principio de idoneidad exige a la autoridad habilitante que no prolongue la medida más allá del tiempo necesario para poder alcanzar el fin perseguido, sin necesidad de apurar los plazo máximos contenidos en la ley. Esta arista del principio de idoneidad resulta especialmente interesante en el ámbito de medidas de investigación tecnológica que nos ocupa, ya que el acceso a los contenido (físicos o remotos) que se encuentren en el dispositivo analizado deberá hacerse en el tiempo imprescindible para garantizar la efectividad de la medida.

---

[47] FJ Vigésimo Segundo de la STC 41/1998, de 24 de febrero (ECLI: ES:TC:1998:41). En el mismo sentido se pronuncia la STC 104/2006, de 3 de abril (ECLI: ES:TC:2006:104).

[48] FJ Octavo de la STS (Sala 2ª) Núm. 484/2015, de 7 de septiembre (ECLI: ES:TS:2015:3981).

c) **Principio de excepcionalidad**

Presentado conjuntamente con el principio de necesidad en el apartado cuarto del artículo 588 bis a), nos encontramos con un principio que no es sino una consecuencia directa de definir las medidas de investigación tecnológica en general, y el registro de los dispositivos de almacenamiento masivo de información en particular, como un medio extraordinario de investigación que conlleva una restricción de derechos fundamentales de la persona; debiendo efectuarse con carácter limitado. Por ello entiende nuestro Alto Tribunal que no debe concederse rutinariamente la concesión de esta medida, pues *"la nota de la excepcionalidad, se completa con las de idoneidad y necesidad y subsidiariedad formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional.*[49]

d) **Principio de necesidad**

Requisito que obliga a que el acceso al dispositivo de almacenamiento sea imprescindible para el buen resultado de la investigación pretendida, no existiendo así otros métodos alternativos que sean menos lesivos de derechos fundamentales pero semejantes en cuanto a su eficacia. Tal y como afirman PEDRAZ PENALVA y ORTEGA BENITO (1990), nos encontramos ante una *"cláusula de subsidiariedad"*, de tal manera que el medio seleccionado para alcanzar el fin no pueda ser suplido por otro igualmente eficaz, pero que no restrinja el derecho fundamental o lo haga de una manera menos gravosa[50].

e) **Principio de proporcionalidad**

Exige finalmente la LECRIM en el apartado quinto del artículo 588 bis a) que la adopción de la medida de investigación sea proporcional al hecho cometido, su gravedad, y la condición del sujeto investigado; de manera que se analice si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés estatal que se trata de salvaguardar[51]. De este modo, la valoración del beneficio para el interés general que supondrá la adopción de la medida considerará parámetros tales como la gravedad del hecho, la trascendencia social del mismo, su producción dentro del ámbito tecnológico, la existencia de indicios o la relevancia del resultado perseguido con la restricción del derecho.

---

[49] FJ Séptimo de la STS (Sala 2ª) Núm. 469/2016, de 31 de mayo (ECLI: ES:TS:2016:2586).

[50] PEDRAZ PENALVA, E. y ORTEGA BENITO, V. (1990). "El principio de proporcionalidad y su configuración en la jurisprudencia del TC y literatura especializada alemanas". *Revista del Poder Judicial (Núm. 17)*, p. 17.

[51] GONZÁLEZ-CUELLAR SERRANO, N. (1990). *Proporcionalidad y derechos fundamentales en el proceso penal.* Madrid. Editorial Colex, p. 225.

Sobre el principio de proporcionalidad existe una muy consolidada doctrina del Tribunal Constitucional que distingue tres aspectos o vertientes para que dicha intromisión resulte proporcional:[52]

(1) Juicio de idoneidad, ya analizado y referente a si la medida es susceptible de conseguir el objetivo propuesto;
(2) juicio de necesidad, también comentado, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia;
(3) Juicio de proporcionalidad en sentido estricto, esto es, si la medida es ponderada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Es en este último criterio señalado por la doctrina constitucional, el de la proporcionalidad en sentido estricto, el que ha quedado plasmado en nuestro apartado quinto del artículo 588 bis a), el cual va a suponer la necesidad de valorar tres ámbitos:

(1) En primer lugar, ***el criterio de la expectativa de las consecuencias jurídicas del delito***, valorando la gravedad de la pena prescrita para el delito que se está investigando.[53]

(2) En segundo lugar, ***el criterio de la importancia de la causa,*** valorando la naturaleza del bien jurídico lesionado, las concretas formas de manifestación del hecho (habitualidad, peligrosidad social, etc.) y las circunstancias relevantes en la persona del investigado, esto es, la tendencia a cometer hechos de la misma naturaleza o la especial intensidad del comportamiento delictivo.[54]

(3) Y por último ***el criterio del grado de imputación,*** es decir, cuando de la instrucción se puedan inferir razones objetivas que permitan afirmar la probabilidad de que se haya cometido un delito.

---

[52] En este sentido la STC (Sala 2ª) Núm. 66/1995, de 8 de mayo (ECLI: ES:TC:1995:66), importó, por primera vez, el calificado como triple test de proporcionalidad, de origen alemán, dando a conocer la fórmula que en adelante empleará el TC para resolver las limitaciones de derechos que se elevaran a su conocimiento. Dicho criterio fue posteriormente empleado, y por su relevancia al presente estudio se mencionan, en las STC 43/2014, de 27 de marzo (ECLI: ES:TC:2014:43); STC 23/2014, de 13 de febrero (ECLI: ES:TC: 2014:23); STC 16/2014, de 30 de enero (ECLI: ES:TC:2014:16); STC 199/2013, de 5 de diciembre (ECLI: ES:TC:2013:199) y STC 173/2011, de 7 de noviembre, *op. cit.;* entre otras.

[53] GONZÁLEZ BEILFUSS, M. (2015). *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional.* Navarra. Editorial Aranzadi, pp. 309-310.

[54] ETXEBERRÍA GURIDI, J.F. (1999). "La inadmisibilidad de los tests masivos de ADN en la investigación de los hechos punibles". *Revista Actualidad Penal (Núm. 28)*, nota 39.

II. DELIMITACIÓN DE LOS DERECHOS FUNDAMENTALES AFECTADOS

Como anteriormente se ha dicho, nuestro Ordenamiento Jurídico contempla la posibilidad de que ciertos trámites sean admitidos en soporte electrónico, de manera que hoy en día la tecnología digital forma parte de nuestra vida profesional. No obstante, el incremento de su uso en el ámbito particular ha conllevado que, actualmente, los dispositivos informáticos y telefónicos sean auténticos diarios digitales que registran y guardan de forma pormenorizada nuestro quehacer diario, lo que en palabras de ZOCO ZABALA, el ordenador, la tableta o el móvil constituyen *"terminales que no albergan sólo comunicaciones a través de medio técnico (videoconferencias, webconferencias, chats o correos electrónicos)"* sino que también contienen *"datos persoanles de tráfico protegidos por el artículo 18.4 CE y documentos personales protegidos por el artículo 18.1 CE"* [55]

Consecuentemente, una investigación que pretenda requisar soportes informáticos o interceptar comunicaciones es susceptible de incidir en la esfera de los derechos fundamentales de los ciudadanos. Es por ello que, una vez sentadas las bases objetivas sobre qué podemos considerar como prueba digital, así como su incardinación dentro de la normativa procesal penal española; como paso previo al análisis del contenido de la diligencia en sí misma, resulta necesario determinar el significado constitucional de algunos derechos fundamentales que la doctrina y la jurisprudencia ha venido considerando afectados con ocasión de la intervención de los dispositivos de almacenamiento masivo de información, puesto que la afectación de dichos derechos fundamentales en la obtención de fuentes de prueba tiene un evidente efecto negativo sobre el proceso: su ilicitud.

Sobre esta casuística inicial, inaugurada por la STC 230/2007, de 5 de noviembre[56], y ratificada posteriormente, entre otras por las STC 115/2013, de 9 de mayo;[57] el máximo interprete constitucional colige que los diferentes supuestos de intervención pueden afectar a derechos tan sumamente esenciales para la personalidad humana contenido en los distintos apartados del artículo 18 CE, tales como el **derecho a las comunicaciones** (en tanto que puedan ser objeto de la diligencia correos electrónicos, mensajes de texto o voz, chat de mensajería instantánea o el registro de llamadas entradas y salientes del terminal); al **derecho al honor y la intimidad** en todo lo relativo a información personal del titular, poseedor o de terceras que pueda almacenarse en el dispositivo (fotografías, vídeos, información médica o de contacto, etc…); **al derecho a la inviolabilidad del domicilio,** en el caso que el acceso al dispositivo tenga lugar dentro del domicilio del investigado o de un tercero. Asimismo, otros derechos aparentemente no afectados

---

[55] ZOCO ZABALA, C. (2015). "Nuevas tecnologías y control de las comunicaciones". *Thomson Reuters-Aranzadi, Cizur Menor*, pp. 45-46.

[56] ECLI: ES:TC:2007:230.

[57] ECLI: ES:TC:2013:115.

como el **derecho a la protección de determinado datos personales**, en el caso que los datos obtenidos se emplearan para fines diferentes a los de la investigación de la presunta comisión de un delito; el **derecho a la propia imagen** en supuestos de captación y/o grabación de videos o fotografías; así como una reciente mención a lo que el Tribunal Supremo considera **"derecho a un propio entorno virtual"**, que más adelante se comentará.

A. Derecho a la intimidad

El derecho fundamental a la intimidad personal y familiar está reconocido tanto en el artículo 8 del CEDH así como en el apartado primero del artículo 18 de la Constitución Española, junto con los derechos fundamentales al honor y la propia imagen. Al tratarse de un derecho personalísimo, del que sólo disfrutan las personas físicas,[58] nos encontramos ante un derecho del que se infiere una doble dimensión (la personal y la familiar) y que no debe ser confundida con el concepto de privacidad.[59]

En el caso concreto analizado en el presente trabajo, que duda cabe que los datos contenidos en un dispositivo electrónico de almacenamiento masivo de almacenamiento de información suponen sin duda alguna una prolongación artificial de nuestra memoria que permite reconstruir un fidedigno retrato-robot de nuestra personalidad, pensamientos, amistades, aficiones, situación financiera e incluso movimientos; de manera que la medida de injerencia que se adopte en el marco de la investigación judicial deberá respetar los precitados principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. El propio TEDH en el caso Lliya Stefanox contra Bulgaria, de 22 de mayo de 2008,[60] ya concluyo que, de acuerdo con el artículo 8.1 del CEDH, la lectura de correos electrónicos y la interceptaciones de conexiones a través de la red de cualquier ciudadano supone una injerencia en su vida probada. En consecuencia, para que en el marco de una investigación criminal dicho derecho pueda ser quebrantado, los ciudadanos deben conocer previamente las circunstancias y condiciones en las que puede realizar dicha injerencia, tal y como ya lo declaró la STEDH del caso Halford contra Reino Unido, de 25 de Junio de 1997.[61]

---

[58] El derecho a la intimidad no es predicable de las personas jurídicas- véase SSTC 124/1985, de 17 de octubre y 69/1999, de 26 de abril- y se extingue con el fallecimiento, vid. STC 231/1988, de 2 de diciembre.

[59] En este sentido autores como GIMENO SENDRA acuden a la teoría de las esferas de los alemanes HUBMANN y SEIDEL, los cuales identifican tres niveles representados como esferas concéntricas, en las que se refieren a ámbitos de mayor o menor envergadura de protección. En el primer anillo externo se encontrarían la esfera pública o información general conocida de la persona; en el segundo los datos personales que la persona difunde a un determinado grupo de personas; y por último la esfera más intima y personal que representa el conjunto de datos sensibles. *Vid.* GIMENO SENDRA, V. (2009), "Las intervenciones electrónicas y la policía judicial", *Diario La Ley, Sección Tribuna, Editorial LA LEY, Núm. 7298, 4 de diciembre de 2009.*

[60] ECLI: CE:ECHR:2008:0522JUD006575501

[61] ECLI: CE:ECHR:1997:0625JUD002060592

Misma conclusión alcanza nuestro Tribunal Constitucional, entre otras en su STC Núm. 173/2011, de 7 de noviembre, al considerar que una intromisión en este tipo de datos contenidos en un dispositivo electrónico afecta claramente al derecho a la intimidad y la esfera personal más íntima del individuo:

> *Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) —por lo que sus funciones podrían equipararse a los de una agenda electrónica—, no sólo forma parte de este mismo ámbito, sino que además* ***a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano****. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona.*[62]

La conclusión, en adelanto a los requisitos legales que deben presidir una medida como es el registro de los dispositivos de almacenamiento masivo de información, no podrá ser otra que la necesidad de existir una resolución judicial habilitante para la irrupción en la esfera más íntima y privada del investigado. Esta resolución, además, deberá tener un contenido propio y que justifique la necesidad y proporcionalidad de la medida; pues de lo que se trata es de abandonar la anterior concepción consistente en que una medida genérica (como la entrada y registro domiciliario o la aprehensión de instrumentos y terminales del investigados) justificaba y sostenía también el análisis de su contenido.

---

[62] FJ Tercero de la STC (Sala 2ª) Núm. 173/2011 (ECLI: ES:TC:2011:173); en el mismo sentido el FJ Quinto de la STC (Sala 1ª) Núm. 170/2013, de 7 de octubre (ECLI: ES:TC:2013:170).

B. Derecho al secreto a las comunicaciones

Sin duda las primeras manifestaciones de lo que se puede considerar como "investigación tecnológica de delitos" las podemos encontrar en la interceptación de correos electrónicos en soporte informático o a través del teléfono móvil. En ambos supuestos, la incautación y posterior análisis de los dispositivos electrónicos que albergan tal información puede afectar al derecho al secreto a las comunicaciones, regulado en los artículos 18.3 de la Constitución Española, así como en los artículos 8 del Convenio Europeo para la protección de los Derechos Humanos, el artículo 12 de la Declaración Universal de los Derechos Humanos y el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos. A partir de esta parca regulación (que carece de un desarrollo legislativo orgánico expreso); se ha permitido construir una estructura de protección del derecho a las comunicaciones por vía fundamentalmente jurisprudencial.[63]

En él se encuentran protegidos de la injerencia de terceros todos los procedimientos de comunicación, con independencia del carácter íntimo o no de su contenido; pues lo esencial es que se trate de un proceso de comunicación entre personas, considerándose en palabras del propio Tribunal Constitucional que "*los mensajes pueden expresarse no solo mediante palabras, sino a través de otro conjunto de signos o señales que componen otras clases de lenguajes",*[64] ya sea mediante el intercambio de caracteres, imágenes, sonidos, señales o incluso emojis.[65]

Siguiendo el excepcional trabajo de ZOCO ZABALA sobre la delimitación de derechos fundamentales en la intervención de los teléfonos móviles[66], determina la autora que el artículo 18.3 CE constituye el objeto de un derecho fundamental que se sustenta tanto en la protección de un espacio (las comunicaciones) que debe ser salvaguardado de la intromisión injustificada de poderes públicos y particulares. Más concretamente lo que se viene a garantizar es la libertad en la comunicación con otras personas, excluyendo a terceros no deseados de la misma, preservando en palabras de DÍEZ PICAZO, *"una esfera de actuación libre de intervención parte de los poderes públicos."* [67]

---

[63] RIDAURA MARTÍNEZ, M.J. (2017). "El legislador ausente del artículo 18.3 de la Constitución (La construcción pretoriana del derecho al secreto de las comunicaciones)" *Revista de Derecho Político UNED* Núm. 100, septiembre-diciembre 2017, p. 350.

[64] Vid. STC 281/2006, de 9 de octubre (ECLI: ES:TC:2006:281).

[65] En este sentido la STS 54/2016, de 10 de mayo (ECLI: ES:TS:2016:1947) analiza un recurso por casación contencioso-disciplinario militar ordinario por una falta leve impuesta por la concurrencia de unos mensajes y emoticonos en el estado de WhatsApp.

[66] ZOCO ZABALA, C. (2013). "Delimitación de derechos fundamentales en la intervención de los teléfonos móviles". *V Congreso Internacional Latina de Comunicación Social. Universidad de La Laguna,* diciembre 2013. Recuperado en:

[67] DIEZ PICAZO, L.M. (2005). *Sistema de derechos fundamentales*. Ed. Cizur Menor. Thomson-Civitas. p. 313.

No obstante, este derecho autónomo que permite la libertad de las comunicaciones y su secreto no es absoluto, pues el propio tenor literal del precepto nos apunta su excepción: salvo resolución judicial. Así la propia norma de 1978 autoriza a intervenir una comunicación, que puede estar contenida en un dispositivo de almacenamiento masivo de información (correos electrónicos, chats, mensajes,…) cuando exista una resolución judicial suficientemente motivada que, aunque en sí misma no constituya una actuación probatoria, pueda conducir como diligencia instructora a la obtención de prueba. Así lo ha entendido el Tribunal Constitucional en su STC (Sala 1ª) Núm. 230/2007, de 5 de noviembre, en la que ha considerado asimilada la exigencia de autorización judicial ex art. 18.3 CE tanto para la **intervención de los correos electrónicos como para la observación de las llamadas entrantes y salientes del titular del teléfono móvil.**[68]

Por último es imprescindible apuntar que parece también superada la doctrina constitucional inaugurada por la STC Núm. 70/2002, de 3 de abril, en la que se circunscribía el derecho al secreto de las comunicaciones solo alcanza "al proceso de comunicación mismo", por lo que una vez concluido *"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".*[69]

Esta teoría estricta del derecho a las comunicaciones ha sido ampliamente criticada por autores como RIVERO SÁNCHEZ-COVISA[70] o RODRÍGUEZ LAINZ[71], quienes consideran que los correos electrónicos abiertos y archivados, así como a los contenidos de mensajería instantánea contenidos en el dispositivo, están sujetos a la garantía constitucional del secreto de las comunicaciones; opinión apoyada sobre la opinión contenida en la STC 230/2007, de 5 de noviembre, al afirmar que:

---

[68] STC (Sala 1ª) Núm. 230/2007, *op. cit.*

[69] En este sentido se ha pronunciado la STC 70/2002, de 3 de abril. LANZAROTE MARTÍNEZ clasifica los correos electrónicos en dos grupos, el primero de ellos compuesto por aquellos mensajes enviados pero no leídos, cuya intercepción sí afecta al derecho al secreto de las comunicaciones y, el segundo, integrado por los correos no enviados o por aquellos enviados, recibidos y leídos, que se enmarcan en la protección del derecho fundamental a la intimidad, en LANZAROTE MARTÍNEZ, P., "Intervenciones de las comunicaciones", Op. Cit., pp. 310-311. La STS 786/2015, de 4 de diciembre, determina que el acceso policial sin autorización policial a programas de mensajería instantánea de un ordenador intervenido no vulneraba el derecho fundamental al secreto de las comunicaciones porque no se inmiscuía en un proceso de comunicación en marcha.

[70] En RIVERO SÁNCHEZ-COVISA, F.J. (2017). *Revisión del concepto constitucional del secreto de las comunicaciones.* Editorial Dykinson, p. 86.

[71] RODRÍGUEZ LAINZ, J.L. (2011) "Los límites a la dimensión formal del derecho al secreto de las comunicaciones". *Diario La Ley, Núm. 7669.*

"[…] bajo la influencia directa ya de la STEDH de 3 de abril de 2007 (caso Copland v. Reino Unido; asunto 62617/00)[…] Realizando un estudio comparativo del caso Copland, concluye que la protección formal va más allá de la finalización de la comunicación, perpetuándose: de suerte que cualquier acceso no consentido por el emisor, destinatario o interlocutor, o que no contara con una previa autorización judicial, supondría una vulneración del artículo 18.3 de la Constitución."

A modo de corolario es interesante concluir que esta distinción pudo tener su interés con anterioridad a la reforma de 2015, toda vez que la distinción en el tratamiento del registro de los contenidos de esta clase de dispositivos generaba no pocos problemas en atención al diferente grado de exigencia que ambos derechos fundamentales requerían para su limitación: autorización judicial en el caso del art. 18.3 CE y no necesidad de la misma en el del art. 18.1 CE. Así, por ejemplo, se venía distinguiendo una diferente naturaleza a los mensajes de correo electrónico según que hubiesen sido ya leídos o no, al entenderse que el proceso comunicativo había finalizado ya en el primer caso y no así en el segundo, no resultando precisa autorización judicial para su incautación en un caso y sí en el otro.[72] Igualmente, se distinguía entre el registro de la agenda de contactos de un teléfono móvil, no necesitada de autorización judicial[73] y la revisión del registro de llamadas entrantes y salientes que, por afectar al derecho fundamental al secreto de las comunicaciones, precisaba de autorización judicial.[74] Esta distinción no obstante ha sido superada, como ya veremos, por el nacimiento de una nueva doctrina jurisprudencial que abordaba de manera unitaria el problema, introduciendo el concepto del "derecho al entorno virtual" como un derecho omnicomprensivo que abarca la protección de la gran diversidad de datos que pueden guardarse en un dispositivo o sistema informático, como puede ser un ordenador.

C. Inviolabilidad del domicilio

Consagrado en el artículo 18.2 de la Carta Magna, así como en los artículos 171 del Pacto Internacional de Derechos Civiles y Políticos de Nueva York, el artículo 8 del Convenio Europeo de Protección de los Derechos Humanos y el artículo 12 de la Declaración Universal de los Derechos Humanos; el derecho a la inviolabilidad del domicilio está íntimamente ligado con el anteriormente analizado derecho a la intimidad, en tanto se trata de una manifestación de éste, al tratarse de un ámbito espacial reservado a su libertad más íntima;[75] sin perjuicio que la jurisprudencia haya equiparado la consideración a la otras circunstancias.

---

[72] STS (Sala 2ª) Núm. 864/2015, de 10 de diciembre (ECLI: ES:TS:2015:5809)

[73] STC (Pleno) Núm. 115/2013, *op. cit.*

[74] STC (Sala 1ª) Núm. 230/2007, *op. cit.*

[75] STC (Sala 2ª) Núm. 94/1999, de 31 de mayo (ECLI: ES:TC:1999:94).

En este sentido, y desde una concepción amplia, lo determinante para la definición del término domicilio es la determinación de un espacio cerrado en el que se desarrolla la vida privada de manera habitual o eventual,[76] de manera que se han venido considerado domicilio la habitación de un hotel (o pensión, hostal o similar),[77] una habitación alquilada,[78] una tienda de campaña,[79] el camarote o zona privada de una embarcación,[80] un domicilio móvil (esto es, roulotte, auto-caravana

[76] Véanse las SSTS (Sala 2ª) Núm. 773/2013, de 22 de octubre (ECLI: ES:TS:2013:5060); STS (Sala 2ª) Núm. 444/2012, de 21 de mayo (ECLI: ES:TS:2012:4189); STS (Sala 2ª) Núm. 861/2011, de 30 de junio (ECLI: ES:TS:2011:5677); STS (Sala 2ª) Núm. 1431/1999, de 13 de octubre (ECLI: ES:TS:1999:6351); STS (Sala 2ª) Núm. 999/1997, de 27 de junio (ECLI: ES:TS:1997:4566).

[77] V*id.* SSTS (Sala 2ª) Núm. 1212/2001, de 22 de junio (ECLI: ES:TS:2001:5386); STS (Sala 2ª) Núm. 1066/2001, de 6 de junio (ECLI: ES:TS:2001:4770); STS (Sala 2ª) Núm. 453/2001, de 16 de marzo (ECLI: ES:TS:2001:2127); STS (Sala 2ª) Núm. 831/2000, de 16 de mayo (ECLI: ES:TS:2000:3929); STS (Sala 2ª) Núm. 1185/1998, de 8 de octubre (ECLI: ES:TS:1998:5733); STS (Sala 2ª) Núm. 1413/1997, de 21 de noviembre (ECLI: ES:TS:1997:7012); y las SSTC (Pleno) Núm. 10/2002, de 17 de enero (ECLI: ES:TC: 2002:10); y STC (Sala 2ª) Núm. 22/1984, de 17 de febrero (ECLI: ES:TC:1984:22).

[78] *Vid.* STS (Sala 2ª) Núm. 352/1996, de 25 de abril (ECLI: ES:TS:1996:2495); si bien la STS (Sala 2ª) Núm. 157/2015, de 9 de marzo (ECLI: ES:TS:2015:1397) no protege una habitación arrendada por ser utilizada con el fin de manipular sustancias tóxicas y no como espacio de vida doméstica.

[79] *Vid.* STS (Sala 2ª) Núm. 379/1996, de 30 de abril (ECLI: ES:TS:1996:2600); STS (Sala 2ª) Núm. 181/1997, de 15 de febrero (ECLI: ES:TS:1997:1041); STS (Sala 2ª) Núm. 1140/1997, de 23 de septiembre (ECLI: ES:TS:1997:5605); STS (Sala 2ª) Núm. 1669/1999, de 19 de mayo (ECLI: ES:TS:1999:7344); STS (Sala 2ª) Núm. 1448/2005, de 18 de noviembre (ECLI: ES:TS:2005:7155).

[80] La jurisprudencia reconoce la protección constitucional de la inviolabilidad del domicilio para las zonas de la embarcación que se puedan estar utilizando como morada o, *in sensu* contrario, la rechaza para las zonas destinadas a otros usos o cuando el barco no constituye un lugar privado asimilable a un domicilio, para lo que utiliza como argumentos el reducido espacio o la ausencia de elementos necesarios para realizar actividades privadas, entre otras en la STS (Sala 2ª) Núm. 513/2014, de 24 de junio (ECLI: ES:TS: 2014:2906); STS (Sala 2ª) Núm. 58/2014, de 6 de febrero (ECLI: ES:TS:2014:481); STS (Sala 2ª) Núm. 169/2011, de 18 de marzo (ECLI: ES:TS:2011:1474); STS (Sala 2ª) Núm. 111/2010 de 24 de febrero (ECLI: ES:TS:2010:966); STS (Sala 2ª) Núm. 932/2009 de 17 de septiembre (ECLI: ES:TS:2009:6230); STS (Sala 2ª) Núm. 151/2009 de 11 de febrero (ECLI: ES:TS:2009:750); STS (Sala 2ª) Núm. 671/2008 , de 22 de octubre (ECLI: ES:TS:2008:6245); STS (Sala 2ª) Núm. 894/2007, 31 de octubre (ECLI: ES:TS:2007:7231); STS (Sala 2ª) Núm. 1009/2006, de 18 de octubre (ECLI: ES:TS:2006:6570); STS (Sala 2ª) Núm. 151/2006, de 20 de febrero (ECLI: ES:TS:2006:717); STS (Sala 2ª) Núm. 919/2004, de 12 de julio (ECLI: ES:TS: 2004:5000); STS (Sala 2ª) Núm. 624/2002, de 10 de abril (ECLI: ES:TS:2002:2529); STS (Sala 2ª) Núm. 1534/1999, de 16 de diciembre (ECLI: ES:TS:1999:8093).

o furgoneta),[81] o un despacho profesional no abierto al público,[82] la parte privada de un negocio,[83] un local de reunión[84] e incluso una cueva[85].

El fundamento de este derecho es obvio: evitar injerencias arbitrarias en el domicilio en el domicilio de una persona, en cuanto se configura como "el ámbito especial donde se proyecta básicamente la intimidad personal y familiar," debiendo quedar excluido éste "del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado."[86]

Como más adelante se analizará, este derecho fundamental también ha sufrido importantes afecciones con la irrupción de las nuevas tecnologías, toda vez que el acceso y registro de determinados instrumentos que se puedan encontrar en un domicilio van a requerir de un acto jurisdiccional habilitante específico, inicialmente requerido por la jurisprudencia[87] y, como veremos, posteriormente incluido en la reforma de la ley procesal penal del 2015.

---

[81] *Vid.* STS (Sala 2ª) Núm. 1165/2009, de 24 de noviembre (ECLI: ES:TS:2009:7014); STS (Sala 2ª) Núm. 158/2003, de 5 de febrero (ECLI: ES:TS:2003:705); STS (Sala 2ª) Núm. 84/2001, de 29 de enero (ECLI: ES:TS:2001:503); y STS (Sala 2ª) Núm. 721/1996, de 18 de octubre (ECLI: ES:TS:1996:5648).

[82] Este supuesto también es conflictivo, pues aunque existen sentencias que admiten la protección de estos espacios de privacidad [por ejemplo la STS (Sala 2ª) de 11 de octubre de 1993 (ECLI: ES:TS:1993:6740)], otras resoluciones afirman que un lugar sólo ocupado durante la jornada laboral no pertenece a su esfera de privacidad protegida por la CE [vid. SSTS (Sala 2ª) Núm. 1406/2003, de 29 de octubre (ECLI: ES:TS: 2003:6699)].

A esta cuestión se añaden mayores matices, como el análisis de si se trata o no de una oficina abierta al [STS (Sala 2ª) Núm. 384/2004, de 22 de marzo (ECLI: ES:TS:2004:1912); o STS (Sala 2ª) de 6 de julio de 1995 (ECLI: ES:TS:1995:3988)]o si se trata de un despacho de un Abogado, cuyo registro puede vulnerar el secreto profesional o el secreto a no declarar del acusado según la jurisprudencia del Tribunal Supremo [STS (Sala 2ª) Núm. 165/2013, de 26 de marzo (ECLI: ES:TS:2013:1649); STS (Sala 2ª) Núm. 974/2012, de 5 de diciembre (ECLI: ES:TS:2012:8701); o STS (Sala 2ª) Núm. 79/2012, de 9 de febrero (ECLI: ES:TS: 2012:414)], del Tribunal Constitucional [STC (Sala 1ª) Núm. 37/1989, de 15 de febrero (ECLI: ES:TC: 1989:37)] y del Tribunal Europeo de Derechos Humanos [SSTEDH Caso Iliya Stefanov, *op. cit.;* Caso Castravet contra Moldavia, de 13 de marzo de 2007 (ECLI: CE:ECHR:2007:0313JUD002339305); Caso Viola contra Italia, de 5 de octubre de 2006 (ECLI: CE:ECHR:2006:1005JUD004510604); Caso Foxley contra Reino Unido, de 20 de junio de 2000 (ECLI: CE:ECHR:2000:0620JUD003327496); o Caso Niemietz contra Alemania, de 16 de diciembre de 1992 (ECLI: CE:ECHR:1992:1216JUD001371088).

[83] Con respecto a la sección privada de un establecimiento público se ha protegido, por ejemplo, una zona privada de una farmacia -la rebotica- en la STS (Sala 2ª) Núm. 576/2002, de 3 de septiembre (ECLI: ES:TS: 2002:5781).

[84] El TS entiende que un local en el que se reunían arrendatarios y amigos para el consumo de hachís es un espacio privado protegido por estar destinado al libre desarrollo de la personalidad. *Vid.* STS (Sala 2ª) Num. 538/1996, de 11 de julio (ECLI: ES:TS:1996:4272).

[85] STS (Sala 2ª) de 19 de octubre de 1994 (ECLI: ES:TS:1994:13875).

[86] STC (Sala 1ª) Núm. 110/1984, de 26 de noviembre (ECLI: ES:TC:1984:110).

[87] STS Núm. 342/2013, de 17 de abril, *op. cit.*

D. Derecho fundamental a la protección de datos

Aunque nos encontramos ante un derecho no reconocido explícitamente en el texto constitucional, desde que el TC se pronunciara en noviembre de 2000 radicalmente a favor de su consideración como *"derecho fundamental autónomo enmarcado en el artículo 18.4 CE,"*[88] podemos considerarlo como un derecho plenamente eficaz, con un desarrollo jurídico propio en la posterior Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En palabras del propio TC, el objeto de protección del derecho fundamental a la protección de datos *"no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal" y que "persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado."*[89]

El derecho a la protección de datos, también conocido como derecho a la autodeterminación informativa o *habeas data,*[90] ha sido definido como la garantía que tiene toda persona física[91] de control y disposición sobre sus datos personales frente a terceros y a los poderes públicos.[92] De

---

[88] SSTC (Pleno) Núm. 290/2000 (ECLI: ES:TC:2000:290) y Núm. 292/2000 (ECLI: ES:TC:2000:292), ambas de 30 de noviembre.

[89] FJ Sexto de la STC 292/2000, de 30 de noviembre, *op. cit.*

[90] GUDÍN RODRÍGUEZ-MAGARIÑOS, F., (2009) "Legalidad de los mecanismos de barrido policial que permiten obtener los números IMEI/ IMSI de las tarjetas de telefonía móvil", *Revista General de Derecho Procesal, Núm. 18, Iustel*, p. 11. Se afirma que el origen de esta expresión tiene su origen en la jurisprudencia alemana, vid. GUERRERO PICÓ, M.C., El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal, Thomson Civitas-Aranzadi, Cizur Menor, 2006, p.187.

[91] No se reconoce para personas jurídicas, según GUERRERO PICÓ, M.C. (2004). *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal.* Tesis doctoral dirigida por Francisco Balaguer Callejón. Universidad de Granada, pp. 222-223.

[92] ORTEGA GIMENEZ, A. y HEREDIA SÁNCHEZ, L.S. (2011). "Los archivos históricos y la protección de datos de carácter personal". *Canelobre: Revista del Instituto Alicantino de Cultura "Juan Gil-Albert" (ejemplar dedicado al cuidado de la memoria. Archivos de la provincia de Alicante),* Núm. 58*;* p. 1.

acuerdo con la clarificadora definición que nos ofrece PÉREZ GIL, el derecho a la protección de datos es *"la facultad de un sujeto de decidir qué es lo que los demás conocen de él".*[93]

En su proceso de conceptualización, algunos autores lo han considerado como una ramificación del derecho a la intimidad o al derecho de acceso a los ciudadanos a los archivos y registros administrativos; lo cierto es que considero más acertada la conceptualización que hacen ORTEGA GIMÉNEZ y GONZÁLEZ MARTÍNEZ como un derecho que sirve a los ciudadanos como garantía sobre el control del uso y destino de la información que pueda afectar a su persona, superando con creces el ámbito de la intimidad de la persona.[94] En similares extremos se ha expresado el Tribunal Constitucional al calificar el derecho a la protección de datos como *"un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»".*[95]

E. Derecho a un entorno virtual

El derecho al propio entorno virtual o derecho a la privacidad del entorno virtual o digital es un derecho de los denominados "de nueva generación" que, en palabras del Tribunal Supremo, protege la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntad o sin ella, va generando el usuario hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos.[96]

---

[93] Vid. PÉREZ GIL, J., "Investigación penal y nuevas tecnologías: algunos de los retos pendientes", Revista Jurídica de Castilla y León, no 7, 2005, p. 227. En un sentido similar, LUCENA CID lo refiere a "la facultad de toda persona para ejercer control sobre la información personal almacenada en medios informáticos tanto por las administraciones públicas como entidades u organizaciones privadas", en LUCENA CID, I.V, "La protección de la intimidad en la era tecnológica: hacia una reconceptualización", Revista internacional de pensamiento político, I época, volumen 7, 2012, p. 135; y GÓMEZ DE LIAÑO FONSECA-HERRERO formula el derecho a la autodeterminación informativa como "el derecho de los ciudadanos a saber quién, cómo y cuándo se tiene información sobre uno mismo; dicho de otro modo, consiste en el derecho a elegir libremente al destinatario de la conversación y al testigo de la esfera privada, con especial cuidado de no incurrir en confusión alguna con el derecho al secreto de las comunicaciones, protector de la comunicación de interferencias de terceros ajenas a ella", en GÓMEZ DE LIAÑO FONSECA-HERRERO, M., "La prohibición constitucional del uso de cámaras ocultas en el marco del denominado periodismo de investigación", Derecom, no 10, Nueva Época, 2012, pp. 10-11.

[94] ORTEGA GIMENEZ, A. y GONZALEZ MARTINEZ, J.A. (2011). "Entidades financieras, privacidad y protección de datos". *Revista Aranzadi de derecho y nuevas tecnologías.* Núm. 25, pp. 36-37.

[95] FJ Cuarto de la STC 292/2000, de 30 de noviembre, *op. cit.*

[96] FJ Séptimo de la STS (Sala 2ª) Núm. 426/2016, de 19 de mayo (ECLI: ES:TS:2016:2149). En el mismo sentido se pronuncian las SSTS (Sala 2ª) Núm. 204/2016, de 10 de marzo (ECLI: ES:TS:2016:1218); Núm. 97/2015, de 24 de febrero (ECLI: ES:TS:2015:823); y Núm. 342/2013, de 17 de abril, *op. cit.*

Sin duda el hecho característico es la protección integral que se otorga a estos datos contenidos en dispositivos tecnológicos diversos que pueden revelar un perfil bastante exacto del investigado, lo que supone un derecho constitucional de nueva generación que ampara de forma unitaria la información que venía protegiéndose de forma separada y con un régimen de protección diferenciado. Será en todo caso la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual.[97]

De este modo nos encontraríamos con un derecho fundamental de creación jurisprudencial que englobaría la información contenida en un dispositivo electrónico pero amparada por diversos derechos tradicionales como la intimidad (sería el caso de fotografías o vídeos contenidos en el dispositivo), el secreto a las comunicaciones (chats de mensajería) o el derecho a la protección de datos (por ejemplo, los datos de geolocalización del dispositivo).

Sin duda la primera manifestación de este nuevo derecho digital la encontramos en la ya mencionada STC Núm. 173/2011, de 7 de noviembre, en la que el máximo intérprete constitución ya vaticinaba que:

> *"(...) los datos personales relativos a una persona individualmente considerados (...) están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano.*
>
> *Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su*

[97] En este sentido, se ratifican la STS Núm. 786/2015, de 4 de diciembre (ECLI: ES:TS:2015:5362); así como las ya citadas SSTS Núm. 426/2016, de 19 de mayo; Núm. 204/2016, de 10 de marzo; Núm. 97/2015, de 24 de febrero; y 342/2013, de 17 de abril.

intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc.
Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona."[98]

Es sobre estos mimbres sobre los que el Tribunal Supremo va a construir y definir algunos de los aspectos de esta nueva garantía para el investigado, principalmente en sus SSTS Núm. 342/2013, de 17 de abril, y Núm. 786/2015, de 4 de diciembre. En la primera de ellas, previa a la reforma operada en 2015 por la LECRIM, ya se posiciona el Alto Tribunal al afirmar:

"la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual".

En el mismo sentido, y ya sobre el paraguas del nuevo marco normativo contenido en el párrafo primero del artículo 588 sexies a), se pronuncia la STS Núm. 786/2015, de 4 de diciembre, al declarar:

"La jurisprudencia de esta Sala ha recordado la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del derecho al entorno digital de todo investigado. Como hemos indicado supra, esa resolución ha de tener un contenido propio, explicativo de las razones por las que, además de la inviolabilidad domiciliaria, se alza la intimidad reflejada en el ordenador. Nuestro sistema no tolera el sacrificio de los derechos proclamados en los apartados 3 y 4 del art. 18 de la CE a partir de una legitimación derivada, de suerte que lo que justifica un sacrificio se ensanche hasta validar implícitamente otra restricción."

[98] STC Núm. 173/2011, de 7 de julio, *op. cit.*

Así pues, el tratamiento unitario de estos datos garantiza la eficacia del registro, en atención a la gran diversidad de datos y archivos que pueden encontrarse en un dispositivo o sistema informático. Así, no sería extraño que se autorizase el acceso a datos íntimos amparados por el art. 18.1 CE y, en el curso del registro, aparecieran comunicaciones relevantes para la investigación amparadas por el art. 18.3 CE.[99] Por ello, la autorización para el registro de un dispositivo o sistema informático en la que se habilite para el acceso a la totalidad del entorno virtual de su usuario, evitará que puedan surgir problemas derivados de la naturaleza del contenido que pudiera ser hallado.

[99] STS Núm. 204/2016, de 10 de marzo, *op. cit.*

III. EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

Analizado el contenido de la reforma operada en 2015, junto con los principios recotres y límites constitucionales que deben presidir la actuación instructora, la nueva redacción de la LECRIM pasa a enumerar una serie de actos de injerencia que no estaban previstos en el texto anterior que, siguiendo la clasificación aportada por ARMENTA DEU, se pueden establecer en dos grandes grupos de tipología de fuentes:[100]

- **los procesos comunicativos,** por un lado, sobre los que recaerán medidas de intervención de las comunicaciones sostenida a través de tecnologías de la información (correo electrónico, WhatsApp y similares o por redes sociales en general) y la propia red pública que sustenta estas comunicaciones.

- **y los dispositivos y sistemas informáticos de almacenamiento de datos**, de otro, consistentes en medidas de acceso y registro para aprehender los datos relevantes contenidos en los mismos; y a la orden de entrega a los depositarios de esos datos, si se trata de información retenida en poder de terceros.

En relación a este segundo grupo, que centra el objeto del presente estudio, hasta la entrada en vigor de la Ley Orgánica 13/2015, de 5 de octubre, la legitimidad en el acceso de este tipo de dispositivos se había fundamentado análogamente en los preceptos relativos al registro de libros, papeles y otros efectos e instrumentos del delito;[101] ahora agrupados en el Capítulo II del analizado Título VIII LECRIM. Ello supuso que hasta la reforma de 2015 toda detención de la correspondencia privada, ya fuera postal, telegráfica o telemática, en el ámbito de la instrucción de delitos, se regía por aplicación de reglas de analogía por el artículo 579 LECRIM, siendo necesarios verdaderos artificios para conseguir unos mínimos requisitos de legalidad de múltiples medidas adoptadas para investigar asuntos, en un contexto social complejo y con una evidente insuficiencia normativa e intentando soslayar entre otros efectos indeseados las condenas de tribunales nacionales e internaciones.

---

[100] Se sigue la clasificación aportada por ARMENTA DEU (2018), *op. cit.* p. 70.

[101] Lo recuerda el FJ Segundo de la STS (Sala 2ª) Núm. 1025/2013, de 26 diciembre (ECLI: ES:TS: 2013:6486), al hacer referencia a la STS (Sala 2ª) Núm. 782/2007, de 3 de octubre (ECLI: ES:TS: 2007:6379).

Con la nueva regulación, tal y como señalan algunos autores, nos encontramos sin duda una de las diligencias más polémicas[102] y rupturistas[103] reguladas en nueva ley procesal penal y que desempeñan un papel destacado y relevante en la instrucción,[104] pues se plantean por primera vez un tratamiento legislativo específico para la inspección de dispositivos de almacenamiento masivo de información.

Como ya se ha apuntado, esta diligencia nace *a priori* como consecuencia directa de un registro domiciliario[105] en el que la policía prevé que en su entrada y registro pueden encontrar ordenadores, móviles o discos duros que pueden ser útiles en el devenir de la instrucción; por lo que la autorización habilitante de la entrada y registro debe considerar también el acceso a tales dispositivos. No obstante, nuestra ley procesal va más allá, permitiendo en ocasiones dicha diligencia fuera del ámbito de un registro domiciliario,[106] siendo necesario en estos casos la puesta en conocimiento del Juez la incautación de tales dispositivos, el cual deberá autorizar expresamente su acceso. Si embargo se prevé también que, apreciado un interés constitucional legítimo[107] dimanante de un caso de urgencia, los agentes de la autoridad podrán llevar a cabo la interceptación e incluso el examen directo del dispositivo; dándole traslado al Juez de instrucción competente dentro del plazo de veinticuatro horas desde que se ejecutó la medida para que sea ratificada o cesada en el plazo de setenta y dos horas.[108]

---

[102] BUENO DE MATA (2015), *op. cit.* p. 1.

[103] Así lo ha definido el propio Tribunal Supremo en su STS (Sala 2ª) Núm. 864/2015, de 10 de diciembre, *op. cit.*, en relación con éste aspecto de la reforma, al afirmar que *"en el artículo 588 sexies a) se lleva a cabo una regulación rupturista, que pretende abandonar prácticas en las que la autorización judicial para la entrada en el domicilio del investigado amparaba cualquier otro acto de injerencia, incluso cuando desbordara el contenido material del derecho reconocido en el art. 18.2 de la CE . Lo que el legislador pretende, por tanto, es que el Juez de instrucción exteriorice de forma fiscalizable las razones que justifican la intromisión en cada uno de los distintos espacios de exclusión que el ciudadano define frente a terceros."*

[104] LÓPEZ-BARAJAS PEREA (2017). "Garantías… *op. cit.* p. 67.

[105] Así se desprende del tenor literal del apartado primero del artículo 588 sexies a) LECRIM al afirmar que "Cuando con ocasión de la práctica de un registro domiciliario sea previsible (…)".

[106] Artículo 588 sexies b) LECRIM.

[107] Definido como causa legítima en el FJ Sexto a. la STC (Sala 1ª) Núm. 25/2005, de 14 de febrero (ECLI: ES:TC:2005:25) cuando expresa que *"el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal."*

[108] Según URBANO CASTRILLO (2008) el legislador ha venido a implementar a nuestro ordenamiento la teoría del fruto del árbol envenenado en la prueba obtenida y se juega con la teoría de conexión antijuricidad, definida ésta como *"una relación entre el medio de prueba ilícito y el reflejo, lo suficientemente fuerte que permita estimar que la ilicitud originaria de la primera trasciende a la segunda, hasta el punto de provocar su sanción invalidante». Por tanto, cuando se diera esa relación fuerte se produce la «contaminación» de la prueba refleja, la cual estaría también afectada por la ilicitud de la primera, y por tanto sería igualmente nula. En este sentido, debemos remitirnos para su mejor comprensión y su relación con las TICs, a dos ejemplos: uno en el que se cumpla está relación de conexidad y otro en el que no." Vid.* URBANO CASTRILLO, E. (2008) "La desconexión de antijuridicidad en la prueba ilícita" *Revista electrónica LegalToday.*

1. Naturaleza de la medida

Es el propio Preámbulo de la Ley 13/2015 el que descarta que los dispositivos de almacenamiento masivo de información puedan ser considerados como simples piezas de convicción, pues su capacidad para recoger y conservar datos de muy diferente índole permite que el acceso a los mismos pueda llegar a afectar de manera intensa a diversos derechos fundamentales y, de ahí, la naturaleza y exigencias de la regulación legal:[109]

> *"La ley pretende acabar con otro vacío normativo. Se trata del registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos. Respecto del primero de ellos, la reforma descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido. Por lo que afecta al registro remoto –diligencia ya presente en buena parte de las legislaciones europeas–, el intenso grado de injerencia que implica su adopción justifica que incluso se refuerce el ámbito objetivo de la medida, para lo que se han acotado con un listado numerus clausus los delitos que la pueden habilitar, y a que se limite la duración temporal, habiéndose optado por una duración de un mes prorrogable como máximo por iguales periodos de tiempo hasta los tres meses."*[110]

Como ha señalado la doctrina, nos encontramos ante un acto de prueba preconstituida del juez de instrucción[111] dado el carácter asegurador de los indicios y fuentes de prueba y, bajo determinadas garantías formales (de entre las que destaca la posibilidad de contradicción) posibilitan su introducción en el juicio oral a través de la lectura como documentos públicos oficiales suficientes para fundar una sentencia de condena. Esto conlleva que los actos de prueba preconstituida tengan una relevancia práctica enorme, ya que se exige que se cumplan todas las garantías que la regulan, debido a que la mayoría de las sentencias penales se fundan, sobre todo, en este tipo de medios de prueba. A la hora de acotar el ámbito objetivo de la medida, del propio tenor literal de la LECRIM ha de entenderse que nos encontramos ante el registro de dispositivos electrónicos que, pudiendo resultar afectados los derechos contenidos en el artículo 18 CE, se realizan en el ámbito de una investigación penal. Por ello, habrán de quedar fuera del ámbito de la regulación otros supuestos como el acceso y registro por parte de los progenitores a los dispositivos de sus hijos o por parte de la empresa en el caso de dispositivos del trabajador.

---

[109] Esta idea deriva de la consideración de los ordenadores como algo más que un instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad del usuario, tal y como ya se había afirmado por el TS en su STS (Sala 2ª) Núm. 342/2013, de 17 de abril, *op. cit.*

[110] Párrafo 14 del Exponendo IV.

[111] LÓPEZ-BARAJAS PEREA (2017). "Garantías… *op. cit.* p. 67.

Asimismo, estas diligencias se caracterizan por estar predominantemente orientadas a la obtención de elementos o datos relacionados con el delito que puedan servir como prueba en el proceso y porque implican, con carácter general, una limitación de ciertos derechos fundamentales.

2. Supuesto ordinarios

2.1. Inicio

Fuera de los casos en los que se exceptúa la orden judicial, y con independencia que nos encontremos en alguno de los supuestos de registro de dispositivos de los precitados artículos sexies a) o b), **el procedimiento se iniciará de oficio por el Juez o a instancias del Ministerio Fiscal o de la Policía Judicial**. En estos casos, la petición de medida de investigación tecnológica habrá de contener, *ex* apartado 2 del artículo 588 bis b), los siguientes elementos:

a) La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos. Dicha descripción deberá ser lo más exhaustiva posible, de manera que se facilite al órgano instructor que debe acordar la medida todos los datos obrantes en la investigación preliminar, siendo imprescindible que no se omitan aquellos datos que puedan afectar relevantemente al resultado de su decisión. Uno de esos datos será, tal y como ha sido reiterada por el Tribunal Supremo, la circunstancia de que con anterioridad a la solicitud de la medida se hubiera solicitado para investigar el mismo delito y ésta hubiera sido rechazada por el juez competente. Por ello, lo que no puede hacer la Policía es, ante la negativa del juez al que inicialmente se le realiza la solicitud, acudir a otro órgano judicial planteándole la misma petición, lo cual ha sido calificado por el Tribunal Supremo como un auténtico fraude de ley, que podría incluso provocar responsabilidades en los funcionarios policiales que así se comportaran.

   En este sentido el Tribunal Constitucional ha venido considerando que no es imprescindible para la validez de la medida que se identifique plenamente al sujeto afectado por la medida, sobre todo en el ámbito de la investigación de delitos tecnológicos, dado que esa exigencia

sería desproporcionada dada la fácil transmisión de la posesión y titularidad de este tipo de dispositivos.[112]

b) La exposición detallada de las razones que justifiquen la necesidad de la medida, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia; no entendiéndose únicamente como suficientes los datos obtenidos en la investigación preliminar, sino también ha de justificarse al organismo instructor por qué la medida que se solicita es idónea, necesaria e imprescindible para poder continuar con la investigación, a fin de que puedan ser evaluados los principios rectores analizados *ut supra.*

c) Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida; debiendo indicar en el oficio los datos de que disponga la policía que permitan, siquiera sea de forma muy aproximada, como corresponde a una fase inicial del proceso, dicha identificación.

d) La extensión de la medida con especificación de su contenido, siendo esencial dicha información para valorar la concurrencia de los requisitos legales para su adopción, pues no siempre serán necesarios todos los datos que se obtendrían del empleo de la diligencia. En el caso concreto de un dispositivo de almacenamiento masivo, habrá que indicar con la mayor precisión qué dispositivo va ser objeto de registro, por ejemplo concretando su ubicación, su usuario, su modelo o marca o cualquier dato que permita individualizar el dispositivo sobre el que la medida se va a aplicar; así como qué aspectos concretos de su contenido son relevantes para la investigación.

---

[112] Así lo ha reiterado el Tribunal Constitucional al no exigir como imprescindible que se identifique al sujeto afectado por la medida STC (Sala 1ª) Núm. 150/2006, de 22 de mayo (ECLI: ES:TC:2006:150) al afirmar que: *"más allá de ello, y aunque en varias sentencias se ha hecho referencia, como expresión del alcance subjetivo de la medida, a la importancia de identificar las concretas personas investigadas, usuarios del teléfono intervenido, del conjunto de la jurisprudencia de este Tribunal, construida fundamentalmente para dar respuesta a casos en que se plantean otro tipo de problemas, no se desprende que la previa identificación de los titulares o usuarios de las líneas telefónicas a intervenir resulte imprescindible para entender expresado el alcance subjetivo de la medida, excluyendo la legitimidad constitucional de las intervenciones telefónicas que, recayendo sobre sospechosos, se orienten a la identificación de los mismos, no otorgan- do relevancia constitucional a cualquier error respecto de la identidad de los titulares o usuarios de las líneas a intervenir. A la vista de los avances tecnológicos en el ámbito de la telefonía –por ejemplo, con la aparición de teléfonos móviles y tarjetas prepago, que dificultan la identificación de los titulares y usuarios, facilitando el intercambio de los teléfonos– esas exigencias resultarían desproporcionadas por innecesarias para la plena garantía del derecho y gravemente perturbadoras para la investigación de delitos graves, especialmente cuando estos se cometen en el seno de estructuras delictivas organizadas".*

A tal efecto, habrá de detallarse en la solicitud de la medida las posibles ubicaciones o directorios sobre los que habrá de extenderse la medida, no siendo admisible una habilitación general abierta para el análisis de un dispositivo electrónico pues, como ya se ha comentado, el acceso a determinados contenidos podría suponer la violación de derechos fundamentales.

e) La unidad investigadora de la Policía Judicial que se hará cargo de la intervención, a fin de que sean conocidos los responsables de su desarrollo a fin de realizar sus funciones de dirección del proceso y de control de la ejecución de la medida así como, en su caso, para exigir la responsabilidades a que hubiera lugar por una inadecuada actuación policial.

f) La forma de ejecución de la medida, lo que variará en función de cuál sea la medida que se trata de utilizar, y que se analizará más adelante.

g) La duración de la medida que se solicita, debiendo motivarse por qué considera necesaria la referida duración, sin perjuicio de que el órgano instructor pueda autorizar la medida por un tiempo inferior si lo considera imprescindible para garantizar el respeto a los principios rectores antes mencionados (especialmente los de necesidad y proporcionalidad).

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con el objeto de dirigir los oportunos oficios judiciales así como para determinar las consecuencias que un eventual incumplimiento o falta de colaboración de esa persona o entidad pueda suponer, que no tendrá por qué coincidir con la unidad investigadora de la Policía Judicial.

2.2. Decisión Judicial: Plazo y contenido

De acuerdo con lo dispuesto en el artículo 588 bis apartado c.1, el Juez de instrucción acordará o desestimará la medida, una vez oído el Ministerio Fiscal, mediante auto motivado en el plazo máximo de 24 horas desde la solicitud. Este plazo, no obstante, podrá ser interrumpido *ex* apartado c.2, si el instructor necesitara requerir al solicitante a fin de aclarar alguno de los requisitos anteriormente detallados. De este modo la autoridad judicial se configura como garante del procedimiento, al menos en los escenarios ordinarios de la medida, es un requisito que ha sido puesto de manifiesto por la jurisprudencia nacional[113] e internacional;[114] toda vez de la diferente naturaleza de los datos que estos dispositivos pueden contener y, por tanto, los múltiples derechos fundamentales que pueden verse atacados.

---

[113] *Vid.* entre otras, las ya citadas SSTS Núm. 204/2016, de 10 de marzo; o la STS (Sala 2ª) Núm. 342/2013, de 17 de abril.

[114] *Vid.* entre otras, la ya comentada STEDH, de 22 de mayo de 2008 (caso Iliya Stefanov contra Bulgaria) y, más recientemente, por el Tribunal Supremo de Estados Unidos, en su sentencia de 25 de junio de 2014 (casos acumulados Riley contra California y Estados Unidos contra Brima Wurie -573 U.S.- 2014).

Asimismo, la necesidad de motivación del auto no es sino una consecuencia directa de una amplia doctrina constitucional que exige que la resolución recoja toda la argumentación que fundamente la autorización,[115] siendo admisible la llamada motivación por remisión siempre que, al ser integrada con la solicitud policial o informe del Fiscal al que se remita, se contengan todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad.[116] En todo caso, resulta esencial que la resolución judicial recoja el juicio de ponderación entre el derecho fundamental afectado y el interés constitucionalmente protegido y sacrificado, del cual se evidencie la necesidad de la adopción de la medida.[117]

En definitiva, la resolución habilitante debe motivar la concurrencia de todos y cada uno de los requisitos o exigencias comunes a las medidas de investigación recogidos en el art. 588 bis c LECRIM, y especialmente el juicio de proporcionalidad; a saber:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.
b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.
c) La extensión de la medida de injerencia, especificando su alcance.
d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.
e) La duración de la medida.
f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.
g) La finalidad perseguida con la medida.

---

[115] *Vid.* STC (Sala 2ª) Núm. 25/2011, de 14 de marzo (ECLI: ES:TC:2011:25); STC (Sala 2ª) Núm. 26/2010, de 27 de abril (ECLI: ES:TC:2010:26); STC (Sala 1ª) Núm. 150/2006, de 22 de mayo, *op. cit.*; STC (Sala 1ª) Núm. 104/2006, de 3 de abril, *op. cit.*; STC (Sala 1ª) Núm. 259/2005, de 24 de octubre (ECLI: ES:TC: 2005:259); STC (Sala 2ª) Núm. 165/2005, de 20 de junio, *op. cit;* STC (Sala 2ª) Núm. 171/1999, de 27 de septiembre (ECLI: ES:TC:1999:171); STC (Sala 1ª) Núm. 49/1996, de 26 de marzo (ECLI: ES:TC:1996:49); o STC (Sala 1ª) Núm. 85/1994, de 14 de marzo (ECLI: ES:TC:1994:85).

[116] En este sentido se pronuncia el FJ Primero de STS (Sala 2ª) Núm. 811/2015, de 9 de diciembre, (ECLI: ES:TS:2015:5213), al afirmar que: *"cuando de infracciones cometidas mediante la utilización de equipos informáticos se trata, la diligencia tendente a su ocupación y al examen de sus contenidos, ha de considerarse como proporcionada, no tanto en función de la pena eventualmente aplicable sino de la propia naturaleza de los hechos investigados, de su mecánica comisiva y de las inevitables necesidades para su ulterior probanza."*

[117] En este sentido lo afirma LÓPEZ-BARAJAS PEREA, I. (2017). "Garantías… *op. cit.* p. 109: *"La excepcional constatación a posteriori de que algunas de esas informaciones podrían no ser exactas o el hecho de que algunos de los mencionados como sospechosos no fueran luego objeto de imputación, no conducen de modo inexorable a la vulneración del derecho. De lo que se trata es de examinar si las sospechas de que el investigado está ejerciendo una actividad criminal, pueden considerarse fundadas. La jurisprudencia habla de «sospechas objetivadas» que han de contar con cierto fundamento en la investigación identificable y susceptible de ulterior contraste65. Se trata de datos objetivos que apoyan tanto la existencia misma del hecho que se pretende investigar, como la relación que tiene el referido hecho con la persona que va a resultar directamente afectada por la medida."*

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Asimismo, y puesto dicho precepto en consonancia con el 588 sexies c LECRIM, se podrían enunciar como requisitos adicionales que debe contener la orden judicial:

i) Los términos y el alcance del registro, considerando la posibilidad de ampliación del registro a otros sistemas informáticos o parte del mismo, cuando existan las suficientes razones para pensar que los datos que se buscan se encuentran almacenados en otro sistema informático o parte de él. La información almacenada en un dispositivo se puede discriminar en atención a su titularidad y a la clase de dato. Como regla general, el registro afectará a datos relativos al sujeto investigado, siendo irrelevante donde se encuentren alojados, esto es, si el dispositivo le pertenece, como será lo habitual, o es de un tercero, salvo que existan razones que justifiquen que el registro recaiga sobre la totalidad de los datos almacenados con independencia de su titularidad.[118]

   Por otro lado y habida cuenta de las distintas clases de datos que pueden encontrarse almacenados en un dispositivo esa especificación puede extenderse también a este aspecto, concretándose el tipo de información a que se puede acceder.[119]

---

[118] En la reciente resolución analizada en la SAP Madrid (Secc. 17ª) Núm. 382/2015, de 21 de mayo (ECLI: ES:APM:2015:6740) analiza esta necesidad de motivación individualizada, en un supuesto donde se plantea la nulidad de la diligencia de volcado del contenido de unas memorias USB intervenidos al acusado, sobre la base de una inexistencia de una resolución que expresamente lo autorice; dado que, aun cuando la mayoría de los dispositivos fueron incautados en el transcurso de una diligencia de entrada y registro, uno de los pen-drives fue aprehendido en un momento posterior, cuando se practicó la detención del investigado.
La Sala considera que, respecto de los dispositivos incautados en el domicilio del investigado existió tal habilitación y que el volcado de la información contenida en los mismos contó con la correspondiente cobertura judicial, ya que, a petición policial, se dictó una resolución judicial autorizando el volcado de la información contenida en los soportes informáticos bajo fe pública del secretario y con entrega de copia a la fuerza actuante para la realización de la pericia. Sin embargo entiende que ha de darse distinto tratamiento al examen efectuado sobre el contenido del pendrive que fue incautado tiempo después con motivo de la detención del acusado. Al respecto afirma que dicho acceso no contaba con ninguna cobertura judicial puesto que su incautación se produjo con posterioridad a la concesión de la autorización inicial y en ningún momento se solicitó su ampliación para el análisis del nuevo dispositivo.
Concluye el Tribunal que, tratándose efectivamente de una medida restrictiva de la intimidad, la autorización no puede entenderse tácitamente concedida y ello determina que, en el caso objeto de análisis, se estime improcedente la valoración de la pericia llevada a cabo sobre el contenido del referido pendrive que quedó al margen del efectivo control judicial De todo ello se desprende que la falta de autorización judicial específica para que los agentes comisionados para la entrada y registro accedan a los dispositivos de almacenamiento masivo relacionados con la actividad delictiva investigada, que puedan ser hallados en el domicilio, va a determinar la nulidad de dicho acceso. Ello sin perjuicio de que la autorización para el examen de los dispositivos electrónicos hallados en el transcurso de la entrada y registro pueda ser concedida por el Juez con posterioridad a la autorización inicial de entrada domiciliaria.

[119] CABEZUDO RODRÍGUEZ, N. (2016). "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *Boletín del Ministerio de Justicia (Núm. 2186)*, pp. 39-47.

j) Las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible la práctica de un eventual dictamen pericial.
k) Opcionalmente, una autorización para realizar copia de los datos informáticos, toda vez que en la medida de lo posible y siempre que las circunstancias lo permitan, es recomendable evitar la incautación de los soportes físicos que contengan los datos y archivos.[120]

2.3. Objeto del registro

Si nos atenemos al tenor literal del artículo 588 sexies a, el objeto de la medida hace referencia a la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital y de acceso a repositorios telemáticos de datos. Dicha vaguedad en la redacción viene a permitir un amplio abanico de posibles dispositivos de almacenamiento susceptibles de aprehensión que excede de los tradicionales instrumentos informáticos cuya función y efecto es precisamente la de guardar o registrar información del usuario a largo plazo (discos externos, memorias USB, CDs, DVDs, memorias digitales, etc.), dejando abierta la puerta a la propia evolución de los sistemas tecnológicos, en la que tendrá cabida cualquier dispositivo capaz de guardar información (aun cuando sea temporal o secundariamente como el caso de los teléfonos móviles, tablets o los dispositivos GPS).

Ello supone que la autorización de la medida deberá tener una previsión esencial: **la localización de la información digital objeto del registro**, toda vez que ésta puede encontrarse en el dispositivo tecnológico físico susceptible de aprehensión o bien en repositorios en la nube, alojados en servidores situados a distancia del usuario (Dropbox, Google Drive, Onedrive o

[120] El tenor literal del art. 588 sexies c.2, el cual declara que *"salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos"*. De esta forma, si la incautación del dispositivo electrónico (soporte físico) puede causar un grave perjuicio a su titular, no se incautará el mismo y se procederá a realizar una copia de los datos garantizando la autenticidad e integridad de los mismos. Entiendo que también es posible la incautación provisional del dispositivo, cuando no pueda realizarse el copiado o volcado de sus datos (con garantía de autenticidad e integridad); pero posteriormente se procederá a su devolución tras la práctica de dicho volcado con condiciones adecuadas.

similares)[121] o bien en los perfiles de redes sociales del usuario.[122] A este respecto parece que va dirigido especialmente el supuesto recogido en el apartado tercero del artículo 588 sexies c), al amparar el acceso a otro sistema informático, sin especificar titularidad propia o ajena del mismo, condicionado siempre a que los datos "sean lícitamente accesibles por medio del sistema inicial o estén disponibles para éste";[123] por lo que consideramos acertada la afirmación de que el legislador ha optado por considerar los repositorios telemáticos de almacenamiento como una parte más del sistema que se registra. Lo realmente determinante no va a ser dónde se encuentren físicamente los datos, sino desde dónde se acceda a ellos. [124]

2.4. Sujetos encargados de la ejecución.

La ejecución de la medida corresponderá generalmente a la Policía Judicial. No obstante, en aras de garantizar el buen desarrollo de la diligencia, el instructor puede ordenar a cualquier persona experta que conozca el funcionamiento del sistema informático, siempre que de ello no se derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.[125]

---

[121] Por eso, el artículo primero del Convenio sobre la Ciberdelincuencia, elaborado en Budapest el 23 de noviembre de 2001, entiende que el sistema informático no es solo el dispositivo aislado en cuestión, sino también el *"conjunto de dispositivos interconectados o relacionados entre sí, que permiten, en la ejecución de un programa, el tratamiento automatizado de datos"*. Así el mencionado Convenio permite ampliar, con ciertas limitaciones, el registro a otros sistemas informáticos cuando existan motivos para pensar que los datos buscados se hallen allí almacenados, exigiéndose también que esos sistemas se encuentren en el territorio español y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para este. También se permite el acceso transfronterizo a los datos almacenados, pero solo cuando se trate de datos de libre acceso al público o con el consentimiento lícito y voluntario de la persona legalmente autorizada para divulgarlos a través de ese sistema informático. Fuera de estos supuestos, la autoridad investigadora debe remitir la correspondiente solicitud de asistencia judicial internacional. Esta petición puede fundamentarse en el propio Convenio de Budapest o bien en otro tratado o instrumento internacional que resulte aplicable.

[122] En este sentido las ya citadas SSTS (Sala 2ª) Núm. 97/2015, de 24 de febrero, y Núm. 342/2013, de 17 de abril; según las cuales el auto judicial por el que se decreta el volcado de datos informáticos contenidos en los ordenadores incautados no permite sin más el acceso a los contenidos de las redes sociales, sino que es preciso acceder a Internet e introducir una clave de usuario, por lo que el apoderamiento del contenido de las redes sociales no se obtiene simplemente por el acceso al contenido del ordenador, sino que se requiere una acción adicional dirigida expresamente a su apertura y examen, siendo necesario el dictado de un nuevo mandamiento judicial.

[123] El acceso resultará lícito siempre que no derive de alguna diligencia de investigación que vulnere derechos fundamentales como sería, por ejemplo, la obtención de las claves de acceso mediante procedimientos fraudulentos. Resultará, sin embargo, lícito, cuando sean reveladas voluntariamente por el investigado [tal es el caso que resuelve la STS (Sala 2ª) Núm. 97/2015, de 24 de febrero, *op. cit.]*; o cuando su averiguación derive de la investigación policial previa al registro, o cuando las claves se hayan obtenido con motivo del registro lícito de los dispositivos del investigado, por ejemplo. En cualquier caso, debe tratarse de repositorios o sistemas informáticos a los que pueda accederse desde el sistema inicial para el que se autorizó el registro.

[124] FISCALÍA GENERAL DEL ESTADO (2019). *Circular 5/2019… op. cit,* p. 39.

[125] De acuerdo al tenor literal del Párrafo 5 del Artículo 588 sexies c.

Esta obligación, que se prevé también respecto de otras medidas de investigación tecnológica,[126] tiene su origen en el informe elaborado por el Consejo Fiscal al Proyecto de Reforma de la Ley de Enjuiciamiento Criminal; el cual consideraba que el artículo 118 CE establece un deber de colaboración para con Jueces y Tribunales que, puesto en relación con la obligación impuesta en el artículo 19.4 de la Convención de Budapest obliga al Estado a adoptar las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias.[127]

De este modo serán sujetos obligados las personas que conozcan el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos, no debiendo ser necesariamente personas con conocimientos técnicos que pudieran proporcionar información sobre el diseño o comportamiento de los sistemas de seguridad; se puede tratar de simples empleados de una empresa, incluso de los niveles jerárquicos más bajos, que dispongan de la información que se busca, como podrían ser las contraseñas de acceso a los datos o la ubicación de éstos dentro de la estructura del sistema informático registrado; así como el fabricante del concreto dispositivo que forme parte del sistema informático que se registra.[128] Esta disposición se completa con el establecimiento de una serie de limitaciones al deber de colaboración, que podrán ser:

- De carácter subjetivo, en el caso de la dispensa de colaborar al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2 LECRIM, no pueden declarar en virtud del secreto profesional, entre las que se encuentra el abogado defensor.[129]

---

[126] Más concretamente para los supuestos de interceptación de las comunicaciones telefónicas y telemáticas, en el artículo 588 ter e), obligando a los prestadores de servicios, operadores de comunicaciones o cualquier persona que contribuya a facilitar las comunicaciones, en los supuestos de utilización de dispositivos o medios técnicos de seguimiento y localización , regulada en el artículo 588 quinquies b.3 obligando a los mismos mencionados en el 588 ter, y en los supuestos relativos a registros remotos, si bien en éste caso extendida también a los responsables del sistema o base de datos que son objeto de la medida en el artículo 588 septies b).

[127] FISCALÍA GENERAL DEL ESTADO (2015). *Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.* Madrid, p. 69.

[128] FISCALÍA GENERAL DEL ESTADO (2019) *Circular 5/2019… op. cit.,* p. 48.

[129] Se ha venido planteando la problemática que plantea este deber de colaboración en situaciones tales como aquella en que el obligado, sin ser investigado propiamente dicho, puede verse afectado por la información contenida en el dispositivo cuyo acceso se pretende con su colaboración. Entiendo que nos encontraríamos plenamente en la exclusión contenida en el apartado 5 respecto de los investigados por cuanto conllevaría una vulneración del derecho a no declarar contra sí mismo, y por tanto a realizar ninguna actividad que pueda provocar una autoincriminación, reconocido en el artículo 24 de la CE y en el artículo 520 de la propia LECRIM.

- De carácter objetivo, en aquellos casos en los que la obligación resulte muy gravosa, empleando el legislador un concepto jurídico indeterminado que preciso interpretar. No obstante, y poniendo dicho concepto en relación con el precedente establecido en el artículo 19.4 del Convenio de Budapest, se podrían considerar casos de obligaciones gravosas: la divulgación de la contraseña u otra medida de seguridad pudiera poner en peligro injustificadamente la vida privada de otros usuarios o de otros datos cuya revisión no ha sido autorizada, o que la facilitación de información supusiera desvelar secretos industriales que pudieran perjudicar una actividad empresarial del afectado.

Por último, se considera intereses aportar la sugerencia efectuada por diversos autores sobre la necesidad que los órganos judiciales encargados de la instrucción reciban una formación específica y permanente sobre las cuestiones relativas a este tipo de operaciones, a fin de no aceptar acríticamente la opinión de los expertos.[130]

2.5. Aprehensión del dispositivo

a) Aprehensión y registro del dispositivo dentro del domicilio del investigado

Como ya se ha indicado, la diligencia sobre almacenamiento masivo de información surge inicialmente en los conflictos que había venido resolviendo la casuística jurisprudencial durante las entradas y registros en lugar cerrado y el posterior análisis de los efectos incautados. Tras la reforma operada, la resolución que autorice la entrada y registro puede acordar el registro de todas las dependencias y pertenencias que allí se encuentren; pero no pueden proceder a acceder al contenido del dispositivo digital encontrado en su interior, tal y como dispone el nuevo artículo 588 sexies a.2 LECRIM:

"La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente."

Por tanto, esta habilitación judicial podrá efectuarse en dos momentos diferentes:

[130] VERDELHO, P. (2009). "La cibercriminalidad y las pruebas electrónicas." *E-Newsletter en la Lucha contra el Crimen (Núm. 1);* citado en LÓPEZ-BARAJAS PEREA, I. (2017). "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos". *Revista de los Estudios de Derecho y Ciencia Política (Núm. 24)*, p.p. 74.

1. **Previamente a la entrada y registro**, de tal manera que el auto habilitante de dicha entrada también autorice de forma expresa el registro de los dispositivos, recogiendo en su fundamentación las razones que justifiquen éste.[131]

2. **Con posterioridad la práctica de la diligencia de entrada**, si en la misma se incautan dispositivos electrónicos y resulta necesario el acceso a su contenido, tal y como lo dispone el artículo 588 sexies a.2 LECRIM. antes transcrito, y sin perjuicio que durante el proceso de entrada y registro los Agentes se encuentren los denominados "hallazgos casuales", es decir, objetos o instrumentos de otras infracciones penales que no son objeto del proceso, lo que requerirá una nueva autorización judicial específica (arts. 588 bis i y 579 bis LECRIM).[132]

Con carácter general, durante la práctica del registro pueden ocuparse aquellos elementos o equipos informáticos que sean necesarios para la investigación o para garantizar la pena de comiso o las responsabilidades pecuniarias que puedan derivarse del delito. De esta manera, puede ser objeto de aprehensión bien el propio dispositivo (y los instrumentos accesorios como pantallas, teclados, ratones, cables y otros similares), o bien únicamente datos o informaciones relevantes para el proceso; aunque con pleno sometimiento a las limitaciones del art. 588 sexies.c.2 LECRIM que se han analizado anteriormente. En cualquier caso, no podemos sino estar de acuerdo con la opinión de BONACHERA VILLEGAS al afirmar que si existen la probabilidad de que las pruebas del delito se encuentren en le dispositivo, lo más adecuado es que el auto de entrada y registro autorice expresamente su registro, debiendo en caso contrario esperar a una resolución posterior que lo habilite.[133]

b) Aprehensión y registro del dispositivo <u>fuera del domicilio del investigado</u>

---

[131] Así se deduce del art. 588 sexies a.1 LECRIM, según el cual *"cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos."*

[132] SÁNCHEZ NÚÑEZ, T. (2007). "Jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal." *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia.* Madrid. Cuadernos de Derecho Judicial editado por el Consejo General del Poder Judicial, p. 271.

[133] BONACHERA VILLEGAS, R. (2012). "El registro de archivos informáticos: una cuestión necesitada de regulación". *Revista General de Derecho Procesal (Núm. 27),* p.6; al entender que *"la orden ha de mencionar los dispositivos que se pretenden recoger y examinar, y razonar, que en ellos se encuentra información sobre el hecho investigado."*

Con anterioridad a la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, la jurisprudencia había venido admitiendo su posibilidad, siempre cuando se cumplieran con los requisitos necesarios para justificarla injerencia en el derecho a la intimidad, aplicando analógicamente las normas del registro en lugar cerrado.[134] Con la nueva redacción, la letra b) del art. 588 sexies regula expresamente estos supuestos en los siguientes términos:

> *"La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización."*

De este modo el legislador ha venido a configurar de manera independiente el registro de los dispositivos de almacenamiento obtenidos fuera del ámbito de las entradas y registro domiciliarias,[135] que aunque el tenor literal parezca afectar únicamente a los supuestos en los que se haya producido la previa aprehensión del dispositivo, solicitándose posteriormente autorización judicial para su registro, no existe inconveniente en interpretar que también resultará aplicable cuando la resolución judicial que preceda a la incautación habilite dicho registro.[136]

Este precepto además deberá ponerse en relación con la facultad que la ley rituaria penal atribuye a la Policía Judicial (art. 282 LECRIM) y al propio Juez de Instrucción (art. 326,1.o LECRIM) pueden recoger aquellos dispositivos que han de ser utilizados como medio de prueba en un proceso penal por contener información relevante para la acreditación de los elementos y circunstancias del delito, debiendo incorporarse al proceso bajo la responsabilidad del Letrado de la Administración de Justicia, o quedarán conservados a disposición judicial en organismo adecuado para su depósito (art. 338 LECRIM).[137]

---

[134] Lo recuerda el FJ Segundo del ATS (Sala 2ª) Núm. 1731/2013, de 26 diciembre (ECLI: ES:TS: 2013:8899A), al hacer referencia al Acuerdo del Pleno no Jurisdiccional de fecha 27 de octubre de 2009.

[135] Por ejemplo, con motivo de una detención en el que la Policía ocupe el teléfono móvil de un sospechoso o el dispositivo de geolocalización de un vehículo implicado en un grave accidente o, en definitiva, el ordenador del investigado en un hecho delictivo.

[136] Así, por ejemplo, cuando se vaya a proceder a la detención de una persona respecto de la que existan sospechas de que porta un teléfono móvil con información relevante para la causa, nada impediría que, en el propio auto de detención o con independencia a este, se resolviera y motivara adecuadamente la procedencia de registrar su teléfono.

[137] DELGADO MARTÍN, J (2016). Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley, Sección Doctrina (Núm. 8693),* p.1.

2.6. Alcance y condiciones del registro

a) Sustanciación en pieza separada

El art. 588 bis d) dispone que la solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

b) Control judicial de la medida

Según el art. 588 bis g), la Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma.

c) Presencia del Letrado de la Administración de Justicia

Aunque la LECRIM guarde silencio expresamente en esta materia,[138] la práctica y la lógica procesal exigen la documentación de la ejecución de la diligencia de registro del dispositivo, documentación que deberá hacer mediante el levantamiento de acta por parte del Letrado de la Administración de Justicia,[139] en la que se detallen las operaciones practicadas y las personas intervinientes. No obstante, la jurisprudencia ha matizado que su intervención no constituye un presupuesto de validez, al considerar que se trata de un proceso *"extremadamente complejo e incomprensible para un profano, pues consiste en el análisis y desentrañamiento de los datos incorporados a un sistema informático".* [140] Por ello a juicio del TS, *"ninguna garantía podría añadirse con la presencia del letrado de la Administración de justicia, al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia. Su presencia sería, de facto, inútil y, por tanto, innecesaria, pues se trata de una técnica en la que el fedatario judicial no es un experto.* Por tanto, lo verdaderamente relevante

---

[138] Así lo sugieren MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. (2015). *La reforma de la Ley de Enjuiciamiento Criminal en 2015.* Madrid. Editorial Castillo de Luna (1ª Edición), p. 375.

[139] Así se desprende de la redacción del párrafo primero del artículo 453.1 LOPJ al establecer que *"Corresponde a los Letrados de la Administración de Justicia, con exclusividad y plenitud, el ejercicio de la fe pública judicial. En el ejercicio de esta función, dejarán constancia fehaciente de la realización de actos procesales en el Tribunal o ante éste y de la producción de hechos con trascendencia procesal mediante las oportunas actas y diligencias."*

[140] Así lo afirma la STS (Sala 2ª) Núm. 256/2008, de 14 de mayo (ECLI: ES:TS:2008:2809) cuando concluye que *"es cierto que esta última actividad - se refiere al análisis de la información de ordenadores incautados en su registro domiciliario autorizado judicialmente- no fue practicada ante el Secretario Judicial, sino por los técnicos policiales en su propia sede. Pero también lo es que, esa presencia que se reclama habría sido, de facto, tan inútil -y, por tanto, innecesaria- como la que pudiera darse en el desarrollo de cualquier otra de las muchas imaginables en cuya técnica el fedatario judicial no fuera experto."*

a efectos de garantizar la validez de la medida no será la presencia del LAJ durante el volcado de datos, sino que *"ya sea mediante la intervención de aquel durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado."*[141] [142] Más reciente ha tenido ocasión el TS de volver a pronunciarse sobre esta cuestión al afirmar que *"la presencia de este fedatario en el acto del volcado de datos no actúa como presupuesto de validez, por cuanto lo decisivo es despejar cualquier duda sobre la integridad de los datos que contenía, garantizar la correlación entre la información aprehendida en el acto de intervención del dispositivo y la que se obtiene en la diligencia de acceso al aparato."* [143]

Sin embargo en este punto es necesario afirmar que no nos encontramos ante una cuestión pacífica, pues no faltan voces que consideran que, aunque la no presencia del LAJ no es una causa de nulidad, sí resultaría conveniente su presencia.[144] Esto se debe a que un volcado practicado sin su presencia dejaría de tener la consideración de prueba preconstituida,[145] pudiendo practicarse sin embargo por otras vías, como la declaración de los sujetos que realizaron el volcado, sin que ello supusiese un merma en las garantías de autenticidad e integridad de la fuente de prueba.[146] Tal es la

---

[141] *Vid.* STS (Sala 2ª,) Núm. 480/2009, de 22 de mayo (ECLI: ES:TS:2009:3057); que a su vez menciona la STS (Sala 2ª,) Núm. 1599/1999, de 15 de noviembre (ECLI: ES:TS:1999:7208) que asimismo manifiesta que *"lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia."*

[142] En este sentido, BONILLA CORREA, J.A. (2015) "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio (1)." *Diario La Ley (Núm. 8522)*, p. 12, al considerar que *"sólo en aquellos casos de intervenciones extremadamente excepcionales, si el Secretario Judicial entiende que su presencia es oportuna, estará presente en el inicio de la diligencia de clonado, por analogía a los dispuesto en el punto sexto de la Instrucción 6/2013 de la Secretaría General de la Administración de Justicia, relativa a La aplicación del Protocolo sobre Aprehensión, análisis, custodia y destrucción de drogas tóxicas, estupefacientes y sustancias psicotrópicas".*

[143] *Vid.* FJ Séptimo de la STS (Sala 2ª) Núm. 187/2015, de 14 de abril (ECLI: ES:TS:2015:1922).

[144] En este sentido VELASCO NÚÑEZ, E. (2013). "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica." *Diario La Ley (Núm. 8183)*, pp. 1001-1012, justifica la necesidad de la presencia del Letrado de la Administración de Justicia, *"como garante de la legalidad, en su misión de velar por la fe pública y la custodia original del efecto tecnológico, que debe después guardar precintado."*

[145] *Vid.* DELGADO MARTÍN, J. (2013) "La prueba electrónica en el proceso penal." *Diario La Ley (Núm. 8167)*, p. 10.

[146] Por ejemplo a través del código hash, que como ya se ha afirmado es el algoritmo que permite afirmar que los datos que se encontraban en el dispositivo en el momento de su ocupación no han sido objeto de manipulación posterior. Por ello, los agentes que realicen el volcado deberán usar elementos técnicos para garantizar la autenticidad e integridad de los datos, que habrán de documentarse para su incorporación al proceso, por lo que lo relevante es la homologación de equipos y programas, tal y como acontece con las pruebas de alcoholemia.

relevancia de la cuestión que ha sido merecedora de adopción de un Acuerdo de la Comisión Nacional de Coordinación de la Policía Judicial[147] en su reunión celebrada el 16 de octubre 2014,[148] cuyo tenor literal se reproduce:

> *"Volcados informáticos: apertura o volcado del disco duro y memoria de almacenamiento de datos de los equipos informáticos ante la presencia del Secretario Judicial. El Excmo. Sr. Fiscal General del Estado manifestó que aunque hay alguna sentencia de la Audiencia Nacional en la que exige la presencia del Secretario Judicial para realizar las operaciones indicadas, el TS, en varias sentencias, deja claro que no es precisa la presencia del Secretario Judicial para los fines indicados. La Comisión Nacional de Policía Judicial por unanimidad estuvo de acuerdo con la propuesta del Comité Técnico, en el sentido de no ser necesaria la presencia del Secretario Judicial para la apertura, volcado de disco duro y memoria de almacenamiento de datos de los equipos informáticos".*

A modo de conclusión apuntar también que, no obstante lo anterior, no ha lugar a duda alguna de que el Letrado de la Administración de Justicia estará siempre presente cuando en el supuesto de que no se proceda a un volcado de datos sino a una copia selectiva de archivos, pues nos encontraríamos ante una selección de información susceptible de contradicción que precisaría una mayor garantía.[149]

d) Presencia del interesado y su abogado

En el caso que la diligencia se practique en unidad de acto con la diligencia de entrada y registro, no plantea duda alguna que habrá que estar a la exigencia del art. 569 LECRIM que determina la necesidad que el interesado o la legítima persona que le represente esté presente;

---

[147] La Comisión Nacional de Coordinación de la Policía Judicial se creó en 1987 con el fin de armonizar y lograr la unidad de la dirección en las fuerzas adscritas a la investigación criminal. Entre sus atribuciones están la de efectuar estudios acerca de la evolución y desarrollo de la delincuencia, emitir informes o realizar propuestas de planes generales de actuaciones de la Policía Judicial contra la criminalidad y unificar criterios o resolver eventuales incidencias que dificulten el adecuado funcionamiento de esta.

[148] Bajo la presidencia del Presidente del CGPJ y del TS, y asistiendo otros miembros de la Comisión como el Ministro de Justicia, el Ministro del Interior, el Fiscal General del Estado, y un vocal del CGPJ.

[149] En este sentido merece la pena citar la SAP Madrid (Secc. 17ª) Núm. 382/2015, de 21 de mayo, *op. cit.*; y la SAP A Coruña (Secc. 6ª) Núm. 268/2013, de 11 de noviembre (ECLI: ES:APC:2013:2875), entre otras.

requisito que solo puede excluirse cuando no resulte posible hacer efectiva su asistencia.[150] Mayores discusiones plantea el caso de aquel registro de dispositivos practicado fuera del ámbito del registro domiciliario, pues nada dice la ley procesal penal en su redacción de 2015, en cuyo texto se han establecido regímenes distintos a la detención y apertura de correspondencia y el registro de dispositivos de almacenamiento masivo de información, sometiendo este último a un régimen que no incluye la presencia del investigado ni de su abogado en su apertura.[151]

Algunas posiciones minoritarias como BONILLA CORREA han venido defendiendo la posibilidad de una aplicación analógica del art. 333 LECRIM, que bajo la rúbrica de la inspección ocular, dentro del título correspondiente a la comprobación del delito y averiguación del delincuente, establece que cuando *"al practicarse las diligencias enumeradas en los artículos anteriores (inspección ocular) hubiese alguna persona declarada procesada, como presunta autora del hecho punible, podrá presenciarlas, ya sola, ya asistida del defensor que eligiese o lo fuese nombrado de oficio, si así lo solicitara."* Este autor entiende que que la diligencia deberá ser notificada a las partes en lo referente al lugar y hora en que se realizará, argumentación que ha sido mayoritariamente rechazada por no resultar de aplicación a la práctica de la diligencia analizada, que claramente no puede calificarse como de inspección ocular.[152]

Por ello, la solución que se ha venido dando mayoritariamente es considerar que la aprehensión de la información contenida en un dispositivo de almacenamiento masivo es meramente funcional, y no se lleva a cabo una selección, sino que se realiza una copia íntegra a fin de realizar una pericia sobre ese contenido. En consecuencia, la presencia del investigado en la

---

[150] *Vid.* STS (Sala 2ª) Núm. 656/2016, de 18 de julio (ECLI: ES:TS:2016:3789); STS (Sala 2ª) Núm. 292/2016, de 7 de abril (ECLI: ES:TS:2016:1545); y STS (Sala 2ª) Núm. 284/2016, de 6 de abril (ECLI: ES:TS:2016:1495). En el FJ Segundo de esta última resolución, el Alto Tribunal concluye que *"ordinariamente el interesado en el registro es el imputado, pues el resultado del registro va a afectar a su defensa , aunque no siempre tiene que estar presente en el registro judicialmente autorizado. El imputado o persona contra la que se dirige el procedimiento puede encontrarse en ignorado paradero, o simplemente fuera de la vivienda y no ser localizable en el momento del registro, ya que la entrada y registro en un domicilio autorizada en el curso de un procedimiento judicial por delito constituye, por su propia naturaleza, una diligencia de carácter urgente que no se puede demorar a la espera de que el imputado regrese a su domicilio o sea localizado policialmente."*

[151] FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO (2016). *Op. cit.,* p. 45 cuando concluye que *"no procede la aplicación analógica de las normas de la LECRIM para la detención y apertura de la correspondencia, que exigen la citación del interesado, a los efectos de que por su abogado se puedan hacer alegaciones e incluso nombrar perito. No siendo tampoco un argumento válido a estos efectos la obsolescencia de la LECRIM con el fin de fundamentar aplicaciones analógicas o extensivas no justificadas de una norma. En los casos de volcados de datos la semejanza –que no la identidad de razón, propia de la analogía-, estribaría en que hay información contenida en un soporte objeto de registro. Sin embargo, el régimen de apertura y examen establecido en los arts. 579 y siguientes LECRIM se funda en que se trata de correspondencia postal o telegráfica, que ha de tener la característica de privada, que físicamente se encuentra dentro de un sobre o similar, y que va a ser examinada por el Juez a fin de tomar conocimiento de lo que interese para la causa, apartando lo demás."*

[152] BONILLA CORREA (2015). *op. cit.*., p. 12.

diligencia de volcado, en cuanto que no se toma ni aparta nada, sino que consiste meramente en la realización de la copia, no se justifica en dotar de mayor garantía a la operación de volcado.[153]

En todo caso, y con el mismo fundamento que exige la presencia del LAJ apuntado en el apartado anterior, cuando se proceda a una copia selectiva de archivos, al no limitarse la diligencia a efectuar un mero proceso técnico de volcado o clonación clonación sino a una selección de información susceptible de contradicción, será también imprescindible la presente del interesado o persona que legítimamente le represente, a fin de garantizar la debida contradicción para garantizar su derecho de defensa.[154]

e) Ausencia de indicaciones en la resolución judicial

De acuerdo a los requisitos ya analizados que debe de contener el auto que autorice el acceso a los dispositivos de almacenamiento masivo, la situación deseable sería que dicha resolución especificara todas y cada una de las condiciones y término de dicha diligencia.[155] No obstante, y dado que en términos prácticos dicha exigencia carecería de sentido, la reiterada jurisprudencia constitucional ha venido señalando que no toda insuficiencia o infracción en la norma procesal penal es relevante a los efectos de suponer una nulidad de actuaciones.*[156]* Por ello, para poder considerar vulnerado algún derecho fundamental en este tipo de diligencias "*no basta con una vulneración meramente formal, sino que es necesario que de esa infracción formal se derive un efecto material de indefensión, con real menoscabo del derecho de defensa y con el consiguiente perjuicio real y efectivo para los intereses del afectado."*[157]

Asimismo en sede procesal no bastará con alegar genérica o abstractamente la indefensión provocada, sino que habrá de concretar los perjuicios efectivos concretos, pues "*no toda infracción procesal es causante de la vulneración del derecho recogido en el arto 24.1 CE, sino que solo alcanza tal relevancia aquella que, por anular las posibilidades de alegación, defensa y prueba*

---

[153] En este sentido se pronuncian las ya comentadas SAP Madrid (Secc. 17ª) Núm. 382/2015, de 21 de mayo , y la SAP A Coruña (Secc. 6ª) Núm. 268/2013, de 11 de noviembre.

[154] *Vid.* FISCALÍA GENERAL DEL ESTADO (2019), *Circular 5/2019… op. cit.,* p. 28.

[155] Resulta paradigmática la STEDH Caso Robathin contra Austria, de 3 de julio de 2012 (ECLI: CE:ECHR:2012:0703JUD003045706), que consideró violado el artículo 8 CEDH en un supuesto de registro de un ordenador de un abogado en el que la medida había permitido el acceso a todos los datos, no sólo a la investigación de la carpeta referida a los clientes objeto de la investigación, al considerar que la resolución autorizante *"dió razones muy breves y bastante generales al autorizar la búsqueda de todos los datos electrónicos del bufete de abogados del solicitante."*

[156] *Vid.* STC (Sala 2ª) Núm. 25/2011, de 14 de marzo, *op. cit.*; STC (Sala 2ª) Num. 164/2005, de 20 de junio (ECLI: ES:TC:2005:164); y STC (Sala 1ª) Núm. 185/2003, de 27 de octubre (ECLI: ES:TC:2003:185).

[157] A título ilustrativo el FJ Tercero de la STC (Sala 1ª) Núm. 185/2003, de 27 de octubre, *op. cit.*

cause una verdadera y real situación de indefensión material."[158] Dicha indefensión, definida junto con la finalidad de los actos procesales mencionada en los artículos 238.3 y 240.1 LOPJ, está íntimamente ligada al mandato del art. 24.1 CE sobre la necesidad de proporcionar al ciudadano la necesaria tutela judicial efectiva que excluya su indefensión y viene caracterizada por una serie de notas características:

- **La necesidad de que se trate de una efectiva y real privación del derecho de defensa**, no existiendo indefensión alguna en aquellos casos en los que no se llega a producir efectivo y real menoscabo del derecho de defensa con el consiguiente perjuicio real y efectivo para los intereses de la parte afectada, bien porque no existe relación sobre los hechos que se quieran probar y las pruebas rechazadas, o bien, porque resulte acreditado que el interesado, pese al rechazo, pudo proceder a la defensa de sus derechos e intereses legítimos.
- La indefensión debe consistir **en un impedimento del derecho a alegar y demostrar en el proceso los propios derechos,**[159] por lo se necesitará una limitación o menoscabo del derecho de defensa en relación con algún interés de quien lo invoca.
- No son admisibles las meras situaciones de expectativa del peligro o riesgo.[160]
- Corresponde la carga de la prueba a la parte que lo alega, debiendo proporcionar un razonamiento adecuado sobre tal extremo, argumentando como se habría alterado el resultado del proceso de haberse evitado la infracción denunciada.[161]

En el caso que nos ocupa, no bastará en consecuencia con denunciar genéricamente la ausencia en la correspondiente resolución que autoriza el registro de las condiciones necesarias para asegurar la integridad de los datos volcados de los servidores y dispositivos de almacenamiento informático y de las garantías para preservarlos. Por el contrario, **será necesario que se determine específicamente cual ha sido la concreta agresión sufrida para con el derecho de defensa que dicho defecto supone, o bien expresar o concretar de otro modo la situación de efectiva indefensión resultante**. Como así ha tenido posibilidad de recalcarlo en numerosas ocasiones el Tribunal Constitucional, el derecho de defensa no puede verse afectado sin más por la falta de una

---

[158] *Vid.* STC (Sala 2ª) Núm. 126/2011, de 18 de julio (ECLI: ES:TC:2011:126); y STC (Sala 2ª) Núm. 122/2007, de 21 de mayo (ECLI: ES:TC:2007:122).

[159] *Vid.* STC (Sala 1ª) Núm. 15/1995, de 24 de enero (ECLI: ES:TC:1995:15); STC (Sala 1ª) Núm. 270/1994, de 17 de octubre (ECLI: ES:TC:1994:270); y STC (Sala 2ª) Núm. 63/1993, de 1 de marzo (ECLI: ES:TC: 1993:63).

[160] *Vid.* STC (Sala 1ª) Núm. 316/1994, de 28 de noviembre (ECLI: ES:TC:1994:316); y STC (Sala 1ª) Núm. 181/1994, de 20 de junio (ECLI: ES:TC:1994:181).

[161] Ello es así porque la situación de indefensión exige la constatación de su material realidad y no solo de su formal confirmación. Tal exigencia es reiterada de modo constante por el Tribunal Constitucional en su STC (Sala 2ª) Núm. 366/1993, de 13 de diciembre (ECLI: ES:TC:1993:366) y STC (Sala 2ª) Núm. 145/1990, de 1 de octubre (ECLI: ES:TC:1990:145); así como por el Tribunal Supremo en la STS (Sala 2ª) Núm. 692/2015, de 3 de noviembre (ECLI: ES:TS:2015:4809); la STS (Sala 2ª) Núm. 814/2014, de 9 de diciembre (ECLI: ES:TS:2014:5068); y la STS (Sala 2ª) Núm. 765/2012, de 27 de septiembre (ECLI: ES:TS:2012:6339).

previa determinación de las precauciones y garantías a adoptar en la toma de datos o en su custodia, sino que lo relevante será analizar si las garantías se han mantenido desde el inicio la ejecución y se mantienen intactas tras la recogida de los datos.[162]

f) Duración del registro y prórrogas

Partiendo de la base del ya analizado principio de proporcionalidad como uno de los principios rectores de las nuevas diligencias tecnológicas en materia de investigación penal; una de sus consecuencias deberá ser que la medida no exceda más del tiempo imprescindible para el esclarecimiento de los hechos o la obtención de la información deseada, lo que deviene en la ya comentada obligación de determinar el alcance temporal concreto que tendrá la medida.

No obstante, a pesar que la nueva redacción ha establecido plazos máximos en función de cada medida concreta,[163] nada dice sobre la duración temporal de el registro de estos dispositivos; lo cual no debe sino entenderse como una consecuencia directa de la obligación impuesta en el párrafo segundo del art. 588 sexies c, dado que el volcado de la información en la mayoría de las ocasiones supone un proceso que no debería dilatarse en el tiempo más allá de unas horas o incluso días en los casos de dispositivos con alta capacidad.

El *dies a quo* plazo empezará a computarse desde que la medida ha sido autorizada, de acuerdo con la reiterada jurisprudencia constitucional que determina que si los efectos se desplegaran sólo y a partir del momento en el que la injerencia efectivamente se realiza se produciría una suspensión individualizada del derecho fundamental durante el tiempo intermedio que transcurre desde el día en que se acuerda la resolución judicial hasta aquél en el que la intervención empieza a producirse.[164]

g) Cese del registro

Al igual que en el apartado anterior respecto al analizado principio de proporcionalidad, así como el de idoneidad, el artículo 588 bis j) dispone que se acordará el cese de la medida *"cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos y, en todo caso, cuando haya transcurrido*

[162] *Vid.* STC (Sala 1ª) Núm. 290/1993, de 4 de octubre (ECLI: ES:TC:1993:290).

[163] En el caso de las intervenciones telefónicas y telemáticas, la duración máxima inicial de la intervención será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses. Una previsión casi idéntica se establece en cuanto a la utilización de dispositivos técnicos de seguimiento y localización. En el caso del registro remoto de equipos informáticos, la ley también limita la duración de la medida al plazo de un mes, prorrogable hasta un máximo de tres meses.

[164] STS (Sala 2ª) Núm. 774/2004, de 16 de junio (ECLI: ES:TS:2004:4188); la STS (Sala 2ª) Núm. 698/2001, de 28 de abril (ECLI: ES:TS:2001:3471); por citar algunas.

*el plazo para el que hubiera sido autorizada",*quedando así determinados cuáles serán los dos límites temporales relativos a este tipo de diligencias tendrán:

- La expiración del plazo que la propia orden judicial determine o llegado el cumplimiento del límite temporal máximo marcado por la ley.
- La ausencia de una causa objetiva que justifique su continuación, una vez constatado que la medida no está dando los resultados esperados o pueden ser utilizados otros medios de investigación menos invasivos de los derechos fundamentales del investigado y con igual eficacia.

h) Ampliación del registro

Sin duda una de las novedades que ha supuesto la reforma operada por la LO 13/2015 ha sido la introducción, por primera vez en nuestro ordenamiento jurídico la posibilidad de extender el registro a otros sistemas conectados con el originariamente investigado. Así, el nuevo artículo 588 sexies 3.c permite la ampliación del registro cuando se tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. En estos casos, se impone una nueva autorización judicial que pondere la necesidad de esa ampliación. No obstante, en caso de urgencia, la policía judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente y, en todo caso, dentro del plazo de veinticuatro horas, de la actuación realizada, de su forma y de su resultado. El juez competente revocará o confirmará la actuación en el plazo de setenta y dos horas.

Esta habilitación, por ejemplo en el caso de un dispositivo móvil o de un ordenador, habilitaría el acceso tanto a los documentos y archivos físicamente en él contenidos, sino también a aquellos programas de comunicación y almacenamiento (Facebook, Whatsapp, Google Drive,…) que se encuentran almacenados en repositorios digitales abiertos desde el dispositivo.

2.7. Efectos del registro

a) Preservación y cadena de custodia de la evidencia

Como se ha analizado anteriormente, el Juez en su resolución deberá prever las medidas destinadas a garantizar la integridad y preservación de los datos para su adecuada valoración por el Tribunal de enjuiciamiento, no solo en los casos en que exista prueba pericial, sino también en los de valoración del dato directamente por el Tribunal; a fin de asegurar que lo que se analiza es justamente lo ocupado y que no ha sufrido alteración alguna, así como garantizando la adecuada

cadena de custodia de los efectos objeto de la pericia, asegurando que son los mismos y con el mismo contenido, que los que fueron intervenidos.[165]

En el caso de la incautación del dispositivo, el medio idóneo e imprescindible para garantizar la identidad de los dispositivos incautados será su adecuada reseña por el Letrado de la Administración de Justicia en el acta que al efecto se levante y que deberá figurar unida al atestado que se presente, el dispositivo incautado, custodiado dentro de una bolsa lacrada por funcionarios policiales o judiciales hasta el momento en que se proceda a su desprecinto ante el LAJ.[166] Cualquier posterior apertura del precinto, como sería la necesaria para llevar a cabo el clonado del dispositivo, deberá hacerse bajo la fe del LAJ; una vez realizado el clonado, el dispositivo deberá ser nuevamente precintado.

En los supuestos en los que no se incaute el dispositivo, dejándolo en poder del investigado, será preciso hacer dos copias; una primera, para garantizar y asegurar el contenido del dispositivo en un momento determinado y una segunda para llevar a cabo sobre ella los análisis que exija la investigación, dejando de esta manera intacta y como muestra de contraste la primera copia, cuya integridad será garantizada por el sellado y custodia de la misma que deberá hacer el LAJ.

Por último, en el caso de que los datos se encuentren almacenados en repositorios externos, también se considera necesario adoptar determinadas garantías o cautelas para asegurar la identidad e integridad de la prueba que pueda resultar de los datos almacenados en repositorios o sistemas informáticos externos; tales como el cambio de claves de acceso por el Juez[167] o la realización de un volcado de la información contenida en el repositorio, con la consecuente consignación por el LAJ.

b) Copia y clonado de los datos

Debido a que la información digital contenida en los dispositivos de almacenamiento masivo de información presenta algunas peculiaridades respecto a la información en papel, el dispositivo intervenido puede necesitar de actuaciones específicas como son la recuperación de archivos borrados u operaciones de desencriptado, que exigen conocimientos especializados, programas específicos y la última tecnología en la materia. Una vez aprehendido el dispositivo, el análisis informático forense de la información en él contenida suele comenzar con la operación de copiado o

---

[165] *Vid.* STC (Sala 2ª) Núm. 170/2003, de 29 de septiembre (ECLI: ES:TC:2003:170) o más recientemente la STS (Sala 2ª) Núm. 1072/2012, de 11 de diciembre (ECLI: ES:TS:2012:9120).

[166] RUBIO ALAMILLO, J. (2018). "Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales" *Diario La Ley Sección Ciberderecho (Núm. 22),* p. 2.

[167] Cumpliendo con ello la previsión contenida en el art. 588 sexies c.1 cuando señala que el Juez *"fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial."*

clonado, que supone la realización de una copia bit a bit del contenido del dispositivo tal y como se encuentra en el momento de la entrada y registro, a un soporte informático (como una memoria USB o un disco duro); garantizando que la información volcada sea una imagen espejo de la original (es decir, exactamente igual a ella, de forma que el análisis no se efectúa sobre el contenido original sino sobre la copia espejo de la misma.

Esta operación resulta clave para el buen devenir de la diligencia, pues como afirma DELGADO MARTÍN,[168] uno de los mayores problemas que plantea la evidencia electrónica es precisamente el relacionado con la cadena de custodia.[169] Esto se debe a que, tratándose de evidencias electrónicas más fácilmente destruibles, alterables o manipulables (voluntariamente o no); resulta absolutamente necesario garantizar que los datos o contenidos que, como evidencias electrónicas, van a ser sometidos al órgano de enjuiciamiento, se corresponden exactamente con los que se encontraban almacenados en los dispositivos incautados.[170]

Esta importancia conlleva que el tratamiento y análisis de tales contenidos **nunca se realizará sobre el contenido original del soporte digital**, sino sobre la copia clonada, de cuyo contenido dará fe el Letrado de la Administración de Justicia en los términos y condiciones ya analizados.[171] Una vez realizado el volcado de la información, se precintará el dispositivo original quedando a disposición el juzgado a fin de que ante cualquier duda que pueda plantearse en el proceso sobre alteración de la prueba, pueda solventarse contrastando la copia sobre la cual se ha trabajado con el original a custodiado en el Juzgado. La garantía de que la copia sobre la que trabaja el perito se corresponde exactamente con el original será proporcionada por la función hash, que otorga al contenido exacto de un archivo un valor numérico único e irrepetible.

---

[168] DELGADO MARTÍN, J (2016) *op. cit.,* p. 11.

[169] Como ha declarado en numerosas ocasiones el TS, a conservación de la cadena de custodia "*es vital para las garantías procesales del investigado, ya que si en un examen forense posterior a la intervención domiciliaria, se detecta que las pruebas o dispositivos informáticos están o pueden estar contaminados, se podría llegar a cuestionar o, incluso, invalidar todo el proceso"*. En este sentido, el FJ Primero de la STS (Sala 2ª) Núm. 987/2012, de 3 de diciembre (ECLI: ES:TS:2012:8316).

[170] En este sentido se expresa RUBIO ALAMILLO, J. (2018) *op. cit.,* p. 2; cuando afirma que, por ejemplo, "*es muy sencillo modificar un mensaje enviado a través de WhatsApp, ya que, para ello, basta únicamente con alterar un registro de la base de datos en que se almacenan estos mensajes, sin que quede rastro alguno de su fecha de modificación o vestigio del mensaje anterior, tal y como fue demostrado por este profesional en un artículo técnico publicado en su página web hace tres años, con una notable repercusión en los medios más importantes del país, tales como el diario El Mundo, la cadena COPE o el Telediario de Televisión Española, así como en medios internacionales. Por impactante que parezca, tres años después, aún es posible manipular los mensajes de WhatsApp sin dejar rastro."*

[171] De ahí que por parte de la doctrina se haya recomendado la presencia del LAJ en la operación de volcado, y así RUBIO ALAMILLO, J. (2018) *Íbid.* p. 3 afirma que *"la garantía de la autenticidad y veracidad del volcado, el LAJ deberá consignar en el acta de volcado, las huellas digitales o códigos hash, de cada uno de los ficheros informáticos resultantes del volcado de la evidencia."*

Estas garantías legales no son más que emanaciones concretas del derecho a un proceso con las garantías debidas,[172] así como del propio derecho fundamental a la defensa,[173] y es que, la verdadera cuestión a dilucidar aquí es la del valor atribuible, desde la perspectiva de su autenticidad, a la prueba electrónica.[174]

c) Incautación de los soportes físicos que contienen los datos

Con carácter general, el apartado segundo del art. 588 sexies c) considera deseable que, a fin de evitar al afectado por el registro perjuicios innecesarios que pudieran derivarse de la incautación de los dispositivos, éstos sean devueltos una vez realizado el clonado, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible dicho clonado a fin de garantizar la autenticidad e integridad de los datos. A dicho precepto general se establecen, no obstante, dos importantes excepciones:

- que los soportes constituyan el objeto del delito, es decir, cuando recaiga sobre él la acción del sujeto activo o resulte afectado directamente por el daño causado por la conducta delictiva o cuando contenga los archivos informáticos de contenido delictivo; siendo en todo caso aplicables las previsiones contenidas en el último párrafo del art. 334 LECRIM.
- que constituyan el instrumento del delito, es decir, cuando hayan sido directamente utilizados como medio para su perpetración; procediéndose siempre su incautación como medida indispensable para llevar a cabo el decomiso que prevén los arts. 127 y siguientes CP.
- Por último se establece una cláusula de cierre general, "otras razones que lo justifiquen", como excepción a la regla general y que deberá ser valorada por el juez en cada caso concreto, ponderándose siempre respecto a los perjuicios que la incautación genere.

d) Presentación del informe pericial

Mediante su informe, que será posteriormente ratificado en el juicio oral, el especialista informático que haya procedido al análisis del dispositivo procederá a describir el sistema de identificación y preservación de la evidencia, así como el procedimiento de volcado de la misma y el resultado del análisis forense, resumiendo todo el procedimiento en unas conclusiones, que serán lo más claras y concisas posibles. Respecto al requisito subjetivo, ya existe jurisprudencia que exige

---

[172] Recogido en el artículo 24.1 de la Constitución Española, así como en diversos instrumentos internacionales de derechos humanos, como la Declaración Universal de Derechos Humanos de 1948 (art. 10 y 11), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (art. 14), la Convención de Derechos de la Infancia de 1989 (art. 40) o el Convenio Europeo de Derechos Humanos de 1950 (art. 6).

[173] Recogido en el artículo 24.2 Constitución Española.

[174] Ya definida en SANCHÍS CRESPO, C. (2012) *op. cit.,* p. 713.

que el informe pericial informático esté firmado por un perito informático con titulación oficial de informática.[175]

e) Utilización de la información en otro procedimiento distinto y descubrimientos casuales:

Tradicionalmente la doctrina se ha enfrentado, en el marco de las actuaciones penales, a un problema respecto a los indicios o pruebas que acreditan la existencia de un delito distinto al investigado (dimensión objetiva) o que puede afectar a un tercero no inicialmente investigado (dimensión subjetiva).[176]

Centrándonos en la primera de ellas, la FISCALÍA GENERAL DEL ESTADO define como hallazgo casual la "aparición de hechos delictivos nuevos en el curso de la investigación de un ilícito penal, no incluidos en la resolución judicial que habilita una medida restrictiva de derechos";[177] debiendo aclararse el valor que esa prueba obtenida puede tener efectos en relación al delito descubierto.

Con carácter previo a la reformar de la LECRIM operada en 2015, el Tribunal Constitucional ya había venido considerando que los hallazgos casuales son válidos,[178] pues en la Constitución no exige, en modo alguno, que el funcionario que se encuentra investigando unos hechos de apariencia delictiva cierre los ojos ante los indicios de delito que se presentaren a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en su investigación oficial, siempre que ésta no sea utilizada fraudulentamente para burlar las garantías de los derechos fundamentales.[179]

Por ello, el legislador ha sido consciente que cualquier medida de investigación relativa a datos íntimos puede revelar, además de la información delictiva buscada, otras diferentes que

---

[175] A título de ejemplo, la STSJ Madrid (Secc. 4ª de lo Social) Núm. 531/2017, de 19 de julio (ECLI: ES:TSJM:2017:9285), en la que se pone de relieve que un título expedido tras realizar un cursillo de una asociación, no es un título oficial de informática que habilite para realizar un informe pericial informático con las debidas garantías.

[176] Siendo la objetiva la que primordialmente ha sido analizada jurisprudencial y doctrinalmente, respecto a a la subjetiva merece la pena destacar que el Tribunal Constitucional se manifestó desfavorable a considerar su admisibilidad en la ya mencionada en este trabajo STC 49/1996, de 26 de marzo, declarando la ilicitud en un caso de intervención telefónica en que aparecen nuevos posibles imputados, sin que se solicitara ampliación de la autorización judicial (pudiendo hacerse, porque había tiempo para ello).

[177] Apartado c) de la Circular de la FISCALÍA GENERAL DEL ESTADO Núm. 1/1999 de 29 de diciembre sobre Enjuiciamiento Criminal. Intervención de las Comunicaciones Telefónicas en el Seno de los Procesos Penales. P. 14.

[178] *Vid.* STS (Sala 2ª) Núm. 740/2012, de 10 de octubre (ECLI: ES:TS:2012:6147).

[179] SSTC (Sala 1ª) Núm. 41/1998, de 31 de marzo, y STC Num. 49/1996, de 26 de marzo, *op. cit*.

aparezcan casualmente; surgiendo el actual art. 588 bis i) que remite directamente a lo dispuesto en el art. 579 bis. Dicho precepto no viene sino a plasmar la reiterada jurisprudencia del Tribunal Supremo que definían cuáles eran los requisitos que habilitarían el uso de una prueba obtenida en un procedimiento distinto:

- En primer lugar será necesario valorarse la legitimidad de la injerencia en el derecho fundamental en el otro proceso en el que se pretende utilizar el material probatorio obtenido en el primero, para lo que se deducirá testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia; así como los antecedentes que justificaron la autorización judicial de ésta, singularmente el oficio policial de solicitud y también la propia resolución judicial habilitante, así como los mismos elementos respecto de las sucesivas prórrogas si las hubiese.

- En segundo lugar se requiere autorización del juez competente, para lo cual éste evaluará el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento; prevenciones estás tendentes a evitar posibles abusos policiales que se producirían cuando, conociendo la policía, o teniendo razones para conocer, que en el curso de la medida investigación iban a descubrirse otros hechos delictivos distintos de aquellos para los cuales dicha medida fue solicitada, sin embargo los funcionarios policiales ocultan dicha información al juez para conseguir, de esta forma irregular, pruebas o indicios de la comisión del delito que realmente pretendían investigar.

- Por último, de acuerdo con el tenor literal del art. 579 bis 3, la decisión sobre la instrucción del delito casualmente descubierto no correspondería al mismo Juez que ha autorizado las medidas de investigación sino al que resulte territorialmente competente, a cuyo efecto establece el artículo que será a dicho juez, cuando se le solicite la autorización preceptiva para continuar con la investigación del delito casualmente descubierto, a quien deberá informársele si las diligencias iniciales en las que dicho descubrimiento se ha producido siguen declaradas secretas, a fin de que tal declaración sea respetada en el nuevo proceso que se inicie, debiéndose comunicar el momento en que dicho secreto se alce. [180]

180 Únicamente resultará necesario incoar un nuevo procedimiento cuando el descubrimiento casual revele un delito heterogéneo al investigado o cuando, en los casos previstos en el art. 17.3 LECRIM, el Ministerio Fiscal no considere conveniente el enjuiciamiento conjunto de los hechos. Cuando se trate de delitos conexos, como ya venía sosteniendo la jurisprudencia, bastará con ampliar el objeto del proceso y de las eventuales diligencias de investigación tecnológica a la investigación del nuevo hecho descubierto. Vid. SSTS (Sala 2ª) Núm. 940/2011, de 27 de septiembre (ECLI: ES:TS:2011:5856); y Núm. 167/2010, de 24 de febrero (ECLI: ES:TS:2010:758).

f) Destrucción de los registros y sus copias

Novedosa y no exenta de crítica doctrinal es sin duda la garantía de conservación que ha impuesto el art. 588 bis k), determinar que una vez que se ponga fin al procedimiento mediante resolución judicial firme (entendida esta como una sentencia, absolutoria o no, o un auto de sobreseimiento libre) se ordenará por la autoridad que haya dictado la resolución el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos informáticos utilizados en la ejecución de la medida, conservándose, no obstante, una copia bajo la custodia del secretario hasta que hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación, a juicio del tribunal.

El problema práctico resulta evidente, pues en no pocas ocasiones dicha copia ocupará un ingente volumen de espacio informático, sin que esté claro para qué dice la ley que se conserve esa copia cuando ya existe una resolución firme que ha puesto fin al procedimiento.

3. Supuestos extraordinarios

Hasta ahora el presente trabajo se ha centrado en aquellos supuestos de intervención y registros amparados en una autorización judicial. Sin embargo, no siempre serán necesarias dichas autorizaciones siempre que haya una afectación de un derecho fundamental,[181] por lo que no será siempre argumento suficiente para postular como presupuesto imprescindible la previa autorización judicial salvo explícita habilitación legal.[182]

3.1. *Intervención policial urgente*

Estable el párrafo cuarto del art. 588 sexies c. LECRIM que *"en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible esta medida (...), la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente y, en todo caso, dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado".*

[181] La Policía Judicial, en algunos casos, podrá actuar de propia autoridad en supuestos en como los cacheos externos, la obligación a expulsar unas bolsas de la boca o la toma de huellas dactilares; donde dichas actuaciones pueden resultar admisibles sin necesidad de una previa validación judicial ni de una ley específica habilitante.

[182] FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO (2016). *op. cit.,* p.49.

De lo anterior podemos destacar cuáles son los requisitos básicos procesales que deben operar para la constitucionalidad de la medida, minuciosamente detallados en la paradigmática STC Núm. 115/2013, de 9 de mayo:[183]

- La urgente necesidad de acceso a los datos.
- La existencia de un interés constitucionalmente legítimo, marcado por:
  + la necesidad de obtener la información, siendo el registro "*estrictamente necesario para la finalidad de la investigación, esto es, solamente podrá acordarse cuando el mismo fin no pueda lograrse por otro medio menos gravoso para el afectado."*[184]
  + la proporcionalidad, al tratarse el registro de *"una medida ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, dada la naturaleza y gravedad del delito investigado y la leve injerencia que comporta en el derecho a la intimidad del recurrente el examen de la agenda de contactos de su teléfono móvil."*[185]
- La posterior comunicación al juez en la forma y plazos que se establecen.
- La convalidación judicial de la medida.

Más recientemente encontramos en la STS Núm. 786/2015, de 4 de diciembre, las notas que se acaban de mencionar, relativas en este caso a un supuesto de urgente intervención policial en relación con imágenes de agresiones sexuales a niñas de cinco y ocho años de edad, razonando que *"la simple posibilidad de que esas imágenes pudieran llegar a convertirse, de una u otra forma, en contenidos difundibles en la red, intensificando de forma irreparable el daño ocasionado a las dos menores, era un riesgo que había de ser ponderado en el momento del juicio de necesidad y proporcionalidad."*[186]

No obstante, como ya se ha referido esta facultad de actuación policial vendrá restringida por la necesidad de que el juez competente, "*también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida."* Con esta previsión no viene sino a incorporarse a la norma procesal penal la reiterada doctrina constitucional que ha venido reiterando que, mientras la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante; es una facultad que es susceptible de control judicial ex post, al igual que el respeto del principio de proporcionalidad. Por ello, si con posterioridad a la medida se constatare por el juez competente la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en

---

[183] STC (Pleno) Núm. 115/2013, de 9 de mayo, *op. cit*.

[184] Párrafo Segundo del FJ Sexto.

[185] Párrafo Séptimo del FJ Sexto.

[186] FJ Primero de la STS Núm. (Sala 2ª) Núm. 786/2015, de 4 de diciembre, *op. cit.*

cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales.[187]

Dicho razonamiento también lo encontramos en el supuesto resuelto por el TC en su STC Núm. 173/2011, en el que un técnico de mantenimiento informático recibió el encargó de reparar el micrófono de un ordenador personal. Finalizada la reparación y a fin de comprobar su buen resultado, decidió aplicar el protocolo habitual, eligiendo al azar diversos archivos para su grabación y posterior reproducción, para lo cual accedió a la carpeta llamada «mis documentos/mis imágenes» del ordenador, donde encontró diversos archivos fotográficos de contenido pedófilo. Tras la denuncia inmediata de los hechos, la policía inmediatamente procedió a comprobar el contenido del disco duro sin solicitar la correspondiente autorización. Concluyó el tribunal que la actuación policial fue legítima, pues *"el sacrificio del derecho fundamental afectado estaba justificado por la presencia de otros intereses constitucionalmente relevantes"*[188]. El TC valoró la conveniencia de que se actuara con rapidez para evitar la destrucción de archivos y comprobar la posible existencia de otros partícipes. También tuvo en cuenta la gravedad de estos hechos, por afectar a menores de edad, esto es, a víctimas especialmente vulnerables.

La anterior conclusión del TC ha levantado críticas en algunos sectores doctrinales minoritarios, [189] quienes entienden que en el caso estudiado no concurría una urgencia y necesidad que legitimara la intervención policial; así como la propia sentencia cuenta con un voto particular formulado por la Magistrada Elisa Pérez Vera en el que se cuestiona si, dado que el ordenador se encontraba en poder de la policía, las diligencias de investigación no podían esperar a que su realización contara con autorización judicial.

---

[187] *Vid.* STC (Sala 1ª) Núm. 206/2007, de 24 de septiembre (ECLI: ES:TC:2007:206) y STC (Sala 1ª) Núm. 70/2002, de 3 de abril (ECLI: ES:TC:2002:70).

[188] FJ Séptimo de la STC (Sala 2ª) Núm. 173/2011, 7 de noviembre, *op. cit.*

[189] CONTRERAS CEREZO, V. (2012). "Internet y la privacidad". *Diario La Ley (Núm. 7819)*, p. 7; cuando afirma que *"no puede compartirse la tesis del Alto Tribunal quien justificó la actuación policial, entre otras causas, en una razón de índole técnico, no tomada en cuenta por los tribunales ordinarios, lo que le está vedado, como era la posibilidad de borrado de los archivos a distancia, riesgo que podía ser conjurado, como afirma el voto particular de la sentencia, con un simple apagado del ordenador"*.

En el mismo sentido se pronuncia ALCÁCER GUIRAO, R. (2012). "Derecho a la intimidad, investigación policial y acceso a un ordenador personal". *La Ley Penal (Núm. 92)*, p. 5, al entender que *"es discutible que las razones esgrimidas permitan justificar la urgente necesidad de intervención policial y no haber recabado la pertinente autorización judicial, pues en el lapso de tiempo en que el Juez de Instrucción hubiera tardado en pronunciarse no había riesgo alguno de destrucción de pruebas o de comisión de nuevos actos delictivos. En este sentido, podría quizá considerarse proporcionada una intervención policial sobre el ordenador que se hubiera limitado a analizar el contenido de la carpeta «Mis documentos», pudiendo entenderse como la mínima actividad de investigación imprescindible para confirmar la verosimilitud de la denuncia. Pero la garantía derivada del art. 18.1 CE imponía a la Policía el mandato de poner en conocimiento de la autoridad judicial el contenido de esa denuncia y —siendo como era necesaria la medida de acceso al ordenador para la averiguación del delito—, solicitar autorización para ello, por lo que, en definitiva, la actuación policial en el presente caso se reveló desproporcionada y lesiva del derecho fundamental"*.

3.2. *Consentimiento del afectado*

La validez de la aceptación voluntaria del interesado, en cuanto a hecho de tratarse como un mecanismo de exclusión personal frente a terceros y a los poderes públicos, ha sido una constante analizada en nuestra doctrinal constitucional; la cual viene recordando que el consentimiento eficaz del sujeto permite la intromisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, por lo que el consentimiento del titular del derecho fundamental legitimará la inmisión en el ámbito de la intimidad e impedirá, por tanto, considerarlo vulnerado.[190]

Este consentimiento deberá ser otorgado por alguien con capacidad para ello[191] y podrá ser revocado en cualquier momento,[192] no pudiendo ser vulnerado más allá del expresado por el propio interesado, no pudiendo quebrarse en palabras del TC "*la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida."*[193] Respecto a la forma en la que dicho consentimiento ha de ser prestado, el TC no ha venido estableciendo rigorísticas formalidades,[194] admitiéndose también un consentimiento tácito del investigado.

Volviendo al caso ya analizado de la STC 173/2011, el TC descartó también la vulneración del derecho a la intimidad al concurrir consentimiento del afectado el cual, pese a no autorizar expresamente el acceso a sus archivos personales donde se encontraban los archivos pedófilos, la conducta del técnico informático no se extralimitó al mandato conferido, añadiendo el Tribunal que avala esta conclusión la circunstancia de que este encargado limitara su actuación a la carpeta "mis documentos" del usuario, mínimo necesario para realizar la referida prueba de grabación, sin pretender adentrarse en otras carpetas respecto de las que, por hallarse más ocultas o por expresarlo así el título asignado a las mismas, pudiera presumirse un mayor revestimiento de protección y reserva. Seguidamente, una vez producido el hallazgo, este se limitó a cumplir con la obligación

---

[190] *Vid.* STC (Sala 2ª) Núm. 173/2011, *op. cit.;* STC (Sala 1ª) Núm. 196/2006, de 3 de julio (ECLI: ES:TC:2006:196); o STC (Sala 1ª) Núm. 83/2002, de 22 de abril (ECLI: ES:TC:2002:83).

[191] STS (Sala 2ª) Núm. 1803/2002, de 4 de noviembre (ECLI: ES:TS:2002:7291).

[192] STC (Sala 2ª) Núm. 159/2009, de 29 de junio (ECLI: ES:TC:2009:159).

[193] FJ Quinto de la STC (Sala 1ª) Núm. 206/2007, de 24 de septiembre, *op. cit.*

[194] En este sentido resolvió la STC (Sala 1ª) Núm. 194/2004, de 15 de noviembre (ECLI: ES:TC:2004:194), al analizar si un reconocimiento médico que se realiza a un trabajador puede afectar a su intimidad personal, reconoce tanto la eficacia del consentimiento prestado verbalmente, como la del derivado de la realización de actos concluyentes que expresen dicha voluntad. Conclusión similar a la que ha llegado el TC en supuestos relativos al derecho a la inviolabilidad del domicilio, considerando que este consentimiento no necesita ser expreso y que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito. [*Vid.* STC (Sala 1ª) Núm. 209/2007, de 24 de septiembre (ECLI: ES:TC:2007:209); y STC (Sala 2ª) Núm. 22/1984, de 17 de febrero (ECLI: ES:TC:1984:22)].

que le viene legalmente impuesta a todo ciudadano consistente en denunciar ante las autoridades competentes la posible perpetración de un delito público del que ha tenido conocimiento.[195]

No ha faltado sin embargo literatura contraria a esta apreciación del TC,[196] al considerar que en ningún modo alguno había mediado consentimiento explícito o tácito a acceder a los archivos personales del ordenador, así como tampoco existió información previa de esta posibilidad de acceso para comprobar el correcto resultado de la reparación.

Cuestión aparte será el **caso en que el consentimiento sea prestado por aquel interesado que se encuentra detenido**, siendo imprescindible para proceder al registro del dispositivo que el consentimiento se preste en presencia de su defensa letrada, lo que así se hará constar por diligencia policial; dado la indubitada afectación que se da al derecho de defensa, por lo que el detenido ha de estar asesorado sobre el contenido y alcance del acto de naturaleza procesal que realiza.[197]

Asimismo presenta alguna particularidad el **caso de equipos informáticos usados por dos o más sujetos**, en el que bastará el consentimiento válido de una de ellas incluso para el examen de datos personales de las otras,[198] siempre y cuando no exista conflicto entre ellas.[199]

Por último mencionar brevemente que, **en aquellos casos donde la aprensión y el registro se realiza por un tercero**, la entrega de la evidencia al investigador oficial se equipara desde el punto de vista del tratamiento probatorio, a la entrega por la víctima, ya que *"además de que el art. 367 LECRIM excluye tercerías sobre los efectos delictivos sólo interesa atender a la garantía de que la ocupación haya sido hecha de buena fe, evitando las provocaciones delictivas y que se pueda explicar la razón de poseer el dispositivo."*[200]

---

[195] Arts. 259 y ss. LECRIM.

[196] *Vid.* RUIZ LEGAZPI, A. (2014). "Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (Incoming de emule) en la STC 173/2011". *Revista Española de Derecho Constitucional (Núm. 100)*, pp. 365-390.

[197] *Vid.* STS (Sala 2ª) Núm. 187/2014, de 10 de marzo, (ECLI: ES:TS:2014:1402); STS (Sala 2ª) Núm. 688/2013, de 30 de septiembre (ECLI: ES:TS:2013:4761); STS (Sala 2ª) Núm. 550/2001, de 3 de abril (ECLI: ES:TS:2001:2769); STS (Sala 2ª) Núm. 1522/1998, de 2 de diciembre (ECLI: ES:TS:1998:7234); o STS (Sala 2ª) Núm. 42/1998, de 23 de enero (ECLI: ES:TS:1998:345); entre otras.

[198] En este sentido se pronuncia el FJ Segundo de la STS (Sala 2ª) Núm. 287/2017, de 19 de abril (ECLI: ES:TS:2017:1487); en el que ante un registro del ordenador utilizado por todo el entorno familiar, el consentimiento válido de uno de sus miembros es suficiente.

[199] *Vid.* STC (Sala 2ª) Núm. 22/2003, de 10 de febrero (ECLI: ES:TC:2003:22).

[200] Supuesto estudiado por la SAP Guadalajara (Sección 1ª) Núm. 8/2016, de 4 de abril (ECLI: ES:APGU:2016:134); en el que un taxista encuentra un móvil olvidado en su coche, que resulta poseer pornografía infantil.

Igual consideración hace el TS en la ya mencionada STS Núm. 864/2015, de 10 de diciembre, al analizar la validez del acceso por parte de una progenitora al contenido de los dispositivos informáticos de su hija menor de edad con las contraseñas que ella conocía, al sospechar que podía ser víctima de alguna actividad ilegal; comunicándose la constatación de este extremo a la policía. La Sala equipara el supuesto a aquellos en los que el interlocutor revela lo que se le comunica por otro bajo compromiso expreso o tácito de confidencialidad o en los que se viola el deber natural de confidencialidad por parte del receptor de una carta privada que desvela la comisión de un delito, afirmando que no se puede hablar aquí de prueba inutilizable. Si la afectación a la intimidad proviene de un particular que está autorizado para acceder a ese ámbito de privacidad, que desvela, aunque abuse de la confianza concedida, no se activa la garantía reforzada del art. 11.1 LOPJ.[201] Idéntico caso al enjuiciado en la STS Núm. 830/2013, de 7 noviembre[202], a raíz de la entrega a la Policía por parte de una madre de su ordenador, cuyo uso compartía con su pareja sentimental, al haber descubierto en él fotos de los pechos y genitales de su hija menor; considerándose que es la persona afectada quien traslada directamente a la Policía el dispositivo del que es titular, donde se almacenan las pruebas del hecho ilícito y justificantes de la denuncia, sin que pueda apreciarse *"vulneración de derecho alguno ya que se trata de una persona con acceso al ordenador, cotitular y por tanto de su uso*" ya que no es la policía quien lleva a cabo el descubrimiento, sino que su función es meramente certificadora.

---

[201] Así el FJ Quinto Párrafo b) de la STS (Sala 2ª) Núm. 864/2015, de 10 de diciembre, *op. cit.* añade que: *"Además estamos hablando de la madre -y no cualquier otro particular-. Es titular de la patria potestad concebida no como poder sino como función tuitiva respecto de la menor. Es ella quien accede a esa cuenta ante signos claros de que se estaba desarrollando una actividad presuntamente criminal en la que no cabía excluir la victimización de su hija. No puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente en que las evidencias apuntaban inequívocamente en esa dirección. La inhibición de la madre ante hechos de esa naturaleza, contrariaría los deberes que le asigna por la legislación civil. Se trataba además de actividad delictiva no agotada, sino viva: es objetivo prioritario hacerla cesar. Tienen componentes muy distintos las valoraciones y ponderación a efectuar cuando se trata de investigar una actividad delictiva ya sucedida, que cuando se trata además de impedir que se perpetúe, más en una materia tan sensible como esta en que las víctimas son menores.)*

[202] STS (Sala 2ª) Núm. 830/2013, de 7 de noviembre (ECLI: ES:TS:2013:5515).

IV. CONCLUSIONES FINALES

I. Las tecnologías de la información y las comunicaciones han cambiado las relaciones sociales en todo el mundo. Por ello, al igual que ocurre con los distintos ámbitos de la vida, conforme dichos procesos se van haciendo más sofisticados, se requieren nuevos instrumentos legales adecuados con tal evolución, no siendo la investigación penal una excepción a esta necesidad de evolución y no pudiendo el derecho quedar al margen de esta evolución. Dicho cambio de paradigma supone que conceptos como "prueba digital", "dispositivo electrónico", "Whatsapp" o "correos electrónicos" son parte del lenguaje habitual de los juzgados españoles hoy en día; por lo que los operadores jurídicos necesitan tener la certeza de cual es el régimen jurídico aplicable a estos nuevos medios y fuentes de prueba; sobre la base de la difusa regulación sobre la prueba existente en nuestro ordenamiento, con referencia supletoria a la legislación procesal civil.

II. Esta actualización de los medios de lucha contra el crimen ha supuesto que junto con las tradicionales medidas de entrada y registro en lugares cerrados, la nueva redacción del Título VIII del Libro II LECRIM va a añadir unos principios rectores que ya venían recogidos en la jurisprudencia recaída en los últimos años en torno a los presupuestos que deben concurrir para toda medida limitativa de un derecho fundamental, que se incluirán junto con las disposiciones comunes a las nuevas medidas de investigación tecnológica en un nuevo Capítulo IV; desarrollándose cada una de ellas en los sucesivos capítulos: interceptación de las comunicaciones telefónicas y telemáticas (Capítulo V); la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (Capítulo VI); la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen (Capítulo VIII); el registro de dispositivos de almacenamiento masivo de información (Capítulo VIII); y los registros remotos sobre equipos informáticos (Capítulo IX).

III. La necesidad de incorporar determinados elementos de investigación en la lucha contra la delincuencia tecnológica no se ha creado *ex profeso* en la última reforma de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015, de 5 de octubre; sino que es la plasmación normativa de una consolidada jurisprudencia nacional e internacional sobre los requisitos y garantías que ha de adoptarse por el órgano instructor. En consecuencia la adopción de cualquier diligencia de investigación tecnológica deberá siempre estar relacionada con el hecho concreto y definido (principio de especialidad); que tanto su duración, objeto y personas que afecte sea adecuado al fin perseguido (principio de idoneidad); que se realice como medida extraordinaria y no sea concebida como un instrumento habitual de investigación (excepcionalidad); que no exista ningún otro método adecuado para obtener el mismo resultado (necesidad); y por último que la medida lesiva sea proporcional al interés que se desee proteger (proporcionalidad).

IV. El respeto a estos principios tiene especial importancia en el marco de la investigación tecnológica debido a la sensibilidad de los datos que pueden encontrarse contenidos en un dispositivo electrónico, tales como gustos, aficiones, opiniones políticas, creencias religiosas o datos de geolocalización. Estos datos, que individualmente considerados no aportarían ningún dato relevante a la instrucción, tomados en conjunto nos permiten generar un "perfil digital" del investigado que pone en tela de juicio determinados derechos fundamentales susceptibles de ser quebrantados.

V. Estas innovaciones técnicas en el procedimiento penal ha de hacerse en riguroso respeto y garantía los derechos y libertades fundamentales de los ciudadanos. En concreto, los datos contenidos en cualquier dispositivo electrónico son susceptibles de 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, respectivamente, datos personales o datos relativos a la comunicación; no siendo relevante el tipo de soporte, físico o electrónico, en el que la información esté alojada ni el hecho, de que el soporte sea un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se accede. En ambos casos nos encontramos ante una injerencia en los aspectos de la esfera más íntima del ser humano; que va a conllevar la necesidad de una habilitación judicial expresa para proceder a dicha intromisión.

VI. Debido a que en la casuística práctica la mayoría de estos dispositivos se encuentran en lugares cerrados, la resolución jurisdiccional habilitante para la invasión del contenido de estos dispositivos electrónicos ha de tener un contenido propio, explicativo de las razones por las que, además de la inviolabilidad domiciliaria, se alza la intimidad reflejada en el ordenador. Se trata, por tanto, de una regulación rupturista, que pretende abandonar prácticas en las que la autorización judicial para la entrada en el domicilio del investigado amparaba cualquier otro acto de injerencia. En definitiva, la entrada y registro en el domicilio del investigado ha de estar debidamente justificada. El instructor habrá de expresar las razones de la necesidad del sacrificio de ese derecho fundamental. Pero tan argumentado como ese acto de injerencia habrá de estar el acceso a los dispositivos de almacenamiento masivo cuya información resulte indispensable para la investigación.

VII. La evidente heterogeneidad de los datos contenidos los dispositivos electrónicos ha supuesto que el Tribunal Supremo se haya decantado por una tesis unitaria de análisis de dichos datos, superando los esfuerzos por diferenciar los derechos fundamentales afectados en función de la naturaleza de cada uno de los contenidos. Ello ha conllevado la conceptualización de un nuevo derecho al propio entorno virtual, que va más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio.

VIII. El supuesto ordinario de la medida, consistente en el análisis y registro de los dispositivos ubicados en lugar cerrado, exigirá la adopción de una resolución judicial expresa que, además de los presupuestos para la entrada y registro, autorice el acceso a la información, estableciendo la descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida; así como un razonamiento sobre la necesidad de la medida, su extensión temporal y objetiva; así como el organismo policial encargado de realizarla.

IX. No será necesaria autorización judicial en dos supuestos concretos: intervención policial urgente o si el investigado voluntariamente lo consiente. En caso de urgencia y concurriendo un interés constitucional legítimo, la Policía Judicial llevará a cabo el registro de dispositivos de almacenamiento masivo de información que podrá alcanzar a cualquier dato íntimo o relativo al secreto de las comunicaciones que integre el derecho al entorno virtual del afectado; debiendo ser convalidado por la autoridad judicial competente en el plazo máximo de 24 horas.

X. Asimismo no será necesaria la resolución judicial habilitante cuando el afectado preste su consentimiento al acceso al dispositivo electrónico, pudiendo ser éste de manera expresa o tácita, aunque siempre de forma inequívoca y libre, sin vicios que la condicionen. Cuando el afectado estuviere detenido, solo será válido el consentimiento otorgado con asistencia letrada.

XI. Como regla general, deberán realizarse copias del contenido de los dispositivos de almacenamiento masivo de información, llevando a cabo el registro y análisis de los datos que contengan sobre las copias y no sobre los originales. La realización de copias deberá ser siempre autorizada previamente por el Juez. No será necesaria la presencia del Letrado de la Administración de Justicia durante el clonado de dispositivos de almacenamiento, aunque sí es recomendable para garantizar la identidad de los dispositivos y su integridad en el caso de copias lógicas o selectivas.

Como regla general deberá evitarse la incautación de los dispositivos de almacenamiento masivo de información salvo en los supuestos previstos en la Ley y, en cualquier caso, adoptarse siempre las cautelas necesarias tendentes a evitar que de la instrucción penal se deriven perjuicios innecesarios para los afectados por la medida de investigación.

BIBLIOGRAFÍA

ABEL LLUNCH, X. y PICÓ I JUNOY, J. (Coord). (2011). *La prueba electrónica.* Barcelona. Editorial Bosch (1ª Edición).

ALCÁCER GUIRAO, R. (2012). "Derecho a la intimidad, investigación policial y acceso a un ordenador personal". *La Ley Penal (Núm. 92)*.

ARMENTA DEU, T. (2018). "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, Whatsapp, redes sociales): entre la insuficiencia y la incertidumbre". *Revista de Internet, Derecho y Política (Núm. 27)*, p.p. 67-79. DOI: http://dx.doi.org/10.7238/idp.v0i27.3149.

BANACLOCHE PALAO, J. (2011) "La prueba en el proceso penal". *Aspectos fundamentales del Derecho Procesal Penal.* Madrid. Editorial La Ley (2.ª Edición).

BONACHERA VILLEGAS, R. (2012). "El registro de archivos informáticos: una cuestión necesitada de regulación". *Revista General de Derecho Procesal (Núm. 27)*.

BONILLA CORREA, J.A. (2015) "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio (1)." *Diario La Ley (Núm. 8522)*.

BORGES BLÁZQUEZ (2018) La prueba electrónica en el proceso penal y el valor probatorio de las conversaciones mantenidas utilizando programas de mensajería instantánea. *Revista Boliviana de Derecho (Núm. 25)*.

BUENO DE MATA, F. (2015). "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". *Diario La Ley (Núm. 8672)*.

CABEZUDO RODRÍGUEZ, N. (2016). "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *Boletín del Ministerio de Justicia* (*Núm. 2186)*.

CONTRERAS CEREZO, V. (2012). "Internet y la privacidad". *Diario La Ley (Núm. 7819)*.

COTINO HUESO, L. (2015). “Algunas cuestiones clave de protección de datos en la nube. Hacia una <regulación nebulosa>”. *Revista catalana de dret públic (Núm. 51)*, pp. 85-103. DOI: 10.2436/20.8030.01.55.

DELGADO MARTÍN, J (2017) La prueba digital. Concepto, clases, aportación al proceso y valoración. *Diario La Ley, Sección Ciberderecho (Núm. 6).*

DELGADO MARTÍN, J (2016) Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley, Sección Doctrina (Núm. 8693).*

DELGADO MARTÍN, J. (2013) “La prueba electrónica en el proceso penal.” *Diario La Ley (Núm. 8167)*.

DICCIONARIO JURÍDICO BÁSICO (2002). Madrid. Editorial Colex. (3ª Edición).

DIEZ PICAZO, L.M. (2005). *Sistema de derechos fundamentales*. Ed. Cizur Menor. Thomson-Civitas.

ETXEBERRÍA GURIDI, J.F. (1999). “La inadmisibilidad de los tests masivos de ADN en la investigación de los hechos punibles". *Revista Actualidad Penal (Núm. 28).*

FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A. (2016). “Registro de dispositivos de almacenamiento masivo de información”. *Dereito: Revista xurídica da Universidade de Santiago de Compostela.* Volumen 25 (Núm. 2)*, p.p. 25-58* DOI: http://dx.doi.org/10.15304/dereito.25.2.3522

FISCALÍA GENERAL DEL ESTADO (2019). *Circular 5/2019, sobre registro de dispositivos y equipos informáticos*. Recuperado en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_5-2019.pdf?idFile=2a2c765e-3a04-4656-87c0-8b56ef73d0b6

FISCALÍA GENERAL DEL ESTADO (2015). *Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas*. Recuperado en: https://www.fiscal.es/documents/20142/fee385a4-e606-4d8c-677a-20605cb1185f

FISCALÍA GENERAL DEL ESTADO (1999). *Circular Núm. 1/1999 de 29 de diciembre sobre Enjuiciamiento Criminal. Intervención de las Comunicaciones Telefónicas en el Seno de los Procesos Penales*. Recuperado en: https://www.fiscal.es/documents/20142/667c2dd9-e80b-0f7b-c761-a3f24d86c701

FUENTES SORIANO, O. (2017). "El valor probatorio de los correos electrónicos", en ASENCIO MELLADO J.M. (Coord.). *El proceso penal ante nuevas formas de delincuencia.* Valencia. Editorial Tirant lo Blanch (1ª Edición).

GARCÍA TORRES M.L. (2011). "La tramitación electrónica de los procedimientos judiciales, según ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil". *Revista Internacional de Estudios de Derecho Procesal y Arbitraje (Núm. 3)*. Recuperado en http://www.riedpa.com/Default.aspx?EdicionID=24

GIMENO SENDRA, V. (2009), "Las intervenciones electrónicas y la policía judicial", *Diario La Ley, Sección Tribuna, Editorial LA LEY, Núm. 7298,* 4 de diciembre de 2009.

GONZÁLEZ BEILFUSS, M. (2015). *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional.* Navarra. Editorial Aranzadi, (1ª Edición).

GONZÁLEZ-CUÉLLAR SERRANO, N. (2008). "Garantías constitucionales de la persecución penal en el entorno digital", en GÓMEZ COLOMER, J. L. (Coord.), *Prueba y proceso penal. Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado.* Valencia. Editorial Tirant lo Blanch (1ª Edición).

GONZÁLEZ-CUELLAR SERRANO, N. (1990). *Proporcionalidad y derechos fundamentales en el proceso penal.* Madrid. Editorial Colex (1ª Edición).

GUDÍN RODRÍGUEZ-MAGARIÑOS, F., (2009) "Legalidad de los mecanismos de barrido policial que permiten obtener los números IMEI/ IMSI de las tarjetas de telefonía móvil", *Revista General de Derecho Procesal, Núm. 18, Iustel.*

GUERRERO PICÓ, M.C. (2004). *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal.* Tesis doctoral dirigida por Francisco Balaguer Callejón. Universidad de Granada.

ILLÁN FERNÁNDEZ, J.M. (2009). *La prueba electrónica, eficacia y valoración en el proceso civil.* Navarra. Editorial Aranzadi (1ª Edición).

LÓPEZ-BARAJAS PEREA, I. (2017). "Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley". *Revista de Derecho Político (Núm. 98)*, p.p. 91-119 .

LÓPEZ-BARAJAS PEREA, I. (2017). "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos". *Revista de los Estudios de Derecho y Ciencia Política (Núm. 24)*, p.p. 64-76. DOI: http://dx.doi.org/10.7238/idp.v0i24.3084

MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. (2015). *La reforma de la Ley de Enjuiciamiento Criminal en 2015*. Madrid. Editorial Castillo de Luna (1ª Edición).

ORTEGA GIMENEZ, A. y GONZALEZ MARTINEZ, J.A. (2011). "Entidades financieras, privacidad y protección de datos". *Revista Aranzadi de derecho y nuevas tecnologías.* Núm. 25.

ORTEGA GIMENEZ, A. y HEREDIA SÁNCHEZ, L.S. (2011). "Los archivos históricos y la protección de datos de carácter personal". Canelobre: Revista del Instituto Alicantino de Cultura "Juan Gil-Albert" (ejemplar dedicado al cuidado de la memoria. Archivos de la provincia de Alicante), Núm. 58.

ORTOÑO ARTÉS, C. (2001). *El avance tecnológico y los nuevos medios de prueba en la LEC. Régimen jurídico de Internet.* Madrid. Editorial La Ley (1ª Edición).

OTAMENDI ZOZAYA, F. (2017). *Las últimas reformas de la Ley de Enjuiciamiento Criminal.* Editorial Dykinson (1ª Edición).

PEDRAZ PENALVA, E. y ORTEGA BENITO, V. (1990). "El principio de proporcionalidad y su configuración en la jurisprudencia del TC y literatura especializada alemanas". *Revista del Poder Judicial (Núm. 17),* p.p. 69-100.

PUJOL CAPILLA, P. (2014). *La nueva prueba documental en la era digital. Su valoración en juicio*. Madrid. Editorial Jurídica Sepín (1ª Edición).

RIDAURA MARTÍNEZ, M.J. (2017). "El legislador ausente del artículo 18.3 de la Constitución (La construcción pretoriana del derecho al secreto de las comunicaciones)". *Revista de Derecho Político UNED Núm. 100, septiembre-diciembre 2017*.

RIVERO SÁNCHEZ-COVISA, F.J. (2017). *Revisión del concepto constitucional del secreto de las comunicaciones.* Editorial Dykinson.

RODRÍGUEZ LAINZ, J.L. (2011) "Los límites a la dimensión formal del derecho al secreto de las comunicaciones". *Diario La Ley, Núm. 7669.*

RUBIO ALAMILLO, J. (2018). "Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales". *Diario La Ley Sección Ciberderecho (Núm. 22).*

RUIZ LEGAZPI, A. (2014). "Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (Incoming de emule) en la STC 173/2011". *Revista Española de Derecho Constitucional (Núm. 100)*, pp. 365-390.

SANCHÍS CRESPO, C. (2012) "La prueba en soporte electrónico". *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio.* Navarra. Editorial Thomson Reuters Aranzadi (1ª Edición).

SÁNCHEZ NÚÑEZ, T. (2007). "Jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal." *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia.* Madrid. Cuadernos de Derecho Judicial editado por el Consejo General del Poder Judicial.

URBANO CASTRILLO, E. (2008) "La desconexión de antijuridicidad en la prueba ilícita". *Revista electrónica LegalToday.* Recuperado en: http://www.legaltoday.com/opinion/articulos-de-opinion/la-desconexion-de-antijuridiciad-en-la-prueba-ilicta

URBANO CASTRILLO, E. y MAGRO SERVET, V. (2003). *La prueba tecnológica en la Ley de Enjuiciamiento Civil*. Navarra. Editorial Aranzadi. (1ª Edición).

VELASCO NÚÑEZ, E. (2013). "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica." *Diario La Ley (Núm. 8183).*

ZOCO ZABALA, C. (2015). "Nuevas tecnologías y control de las comunicaciones". *Thomson Reuters-Aranzadi, Cizur Menor,* pp. 45-46.

ZOCO ZABALA, C. (2013). "Delimitación de derechos fundamentales en la intervención de los teléfonos móviles". *V Congreso Internacional Latina de Comunicación Social. Universidad de La Laguna, D*iciembre 2013. Recuperado en: http://www.revistalatinacs.org/13SLCS/2013_actas/049_Zoco.pdf

JURISPRUDENCIA

I. TRIBUNAL CONSTITUCIONAL

Resolución	Sala/Sección	Número	Fecha	ECLI
Sentencia	Sala 5ª	54/2016	10/05/2016	ES:TS:2016:1947
Sentencia	Sala 2ª	145/2014	22/09/2014	ES:TC:2014:145
Sentencia	Sala 1ª	43/2014	27/03/2014	ES:TC:2014:43
Sentencia	Pleno	23/2014	13/02/2014	ES:TC:2014:23
Sentencia	Pleno	16/2014	30/01/2014	ES:TC:2014:16
Sentencia	Pleno	199/2013	05/12/2013	ES:TC:2013:199
Sentencia	Sala 1ª	170/2013	07/10/2013	ES:TC:2013:170
Sentencia	Pleno	115/2013	09/05/2013	ES:TC:2013:115
Sentencia	Pleno	222/2012	27/11/2012	ES:TC:2012:222
Sentencia	Sala 2ª	173/2011	07/11/2011	ES:TC:2011:173
Sentencia	Sala 2ª	126/2011	18/07/2011	ES:TC:2011:126
Sentencia	Sala 2ª	25/2011	14/03/2011	ES:TC:2011:25
Sentencia	Sala 2ª	26/2010	27/04/2010	ES:TC:2010:26
Sentencia	Sala 2ª	159/2009	29/06/2009	ES:TC:2009:159
Sentencia	Pleno	12/2008	29/01/2008	ES:TC:2008:12
Sentencia	Sala 1ª	230/2007	05/11/2007	ES:TC:2007:230
Sentencia	Sala 1ª	206/2007	24/09/2007	ES:TC:2007:206
Sentencia	Sala 1ª	209/2007	24/09/2007	ES:TC:2007:209
Sentencia	Sala 2ª	122/2007	21/05/2007	ES:TC:2007:122
Sentencia	Sala 1ª	281/2006	09/10/2006	ES:TC:2006:281
Sentencia	Sala 1ª	253/2006	11/09/2006	ES:TC:2006:253
Sentencia	Sala 1ª	196/2006	03/07/2006	ES:TC:2006:196
Sentencia	Sala 1ª	150/2006	22/05/2006	ES:TC:2006:150
Sentencia	Sala 1ª	104/2006	03/04/2006	ES:TC:2006:104
Sentencia	Sala 2ª	26/2006	30/01/2006	ES:TC:2006:26
Sentencia	Sala 1ª	259/2005	24/10/2005	ES:TC:2005:259
Sentencia	Sala 2ª	165/2005	20/06/2005	ES:TC:2005:165
Sentencia	Sala 2ª	164/2005	20/06/2005	ES:TC:2005:164

Resolución	Sala/Sección	Número	Fecha	ECLI
Sentencia	Sala 1ª	25/2005	14/02/2005	ES:TC:2005:25
Sentencia	Sala 1ª	194/2004	15/11/2004	ES:TC:2004:194
Sentencia	Sala 1ª	185/2003	27/10/2003	ES:TC:2003:185
Sentencia	Pleno	184/2003	23/10/2003	ES:TC:2003:184
Sentencia	Sala 2ª	170/2003	29/09/2003	ES:TC:2003:170
Sentencia	Sala 2ª	22/2003	10/02/2003	ES:TC:2003:22
Sentencia	Sala 1ª	83/2002	22/04/2002	ES:TC:2002:83
Sentencia	Sala 1ª	70/2002	02/04/2002	ES:TC:2002:70
Sentencia	Sala 2ª	169/2001	16/07/2001	ES:TC:2001:169
Sentencia	Pleno	10/2002	17/01/2001	ES:TC:2002:10
Sentencia	Pleno	292/2000	30/11/2000	ES:TC:2000:290
Sentencia	Pleno	290/2000	30/11/2000	ES:TC:2000:292
Sentencia	Sala 2ª	171/1999	27/09/1999	ES:TC:1999:171
Auto	Sección 4ª	219/1999	17/09/1999	ES:TC:1999:219A
Sentencia	Sala 2ª	94/1999	31/05/1999	ES:TC:1999:94
Sentencia	Sala 1ª	41/1998	31/03/1998	ES:TC:1998:41
Sentencia	Sala 1ª	49/1996	26/03/1996	ES:TC:1996:49
Sentencia	Sala 1ª	207/1996	22/01/1996	ES:TC:1996:207
Sentencia	Sala 2ª	66/1995	08/05/1995	ES:TC:1995:66
Sentencia	Sala 1ª	15/1995	24/01/1995	ES:TC:1995:15
Sentencia	Sala 1ª	316/1994	28/11/1994	ES:TC:1994:316
Sentencia	Sala 1ª	270/1994	17/10/1994	ES:TC:1994:270
Sentencia	Sala 1ª	181/1994	20/06/1994	ES:TC:1994:181
Sentencia	Sala 1ª	85/1994	14/03/1994	ES:TC:1994:85
Sentencia	Sala 2ª	366/1993	13/12/1993	ES:TC:1993:366
Sentencia	Sala 1ª	290/1993	04/10/1993	ES:TC:1993:290
Sentencia	Sala 2ª	63/1993	01/03/1993	ES:TC:1993:63
Sentencia	Sala 2ª	145/1990	01/10/1990	ES:TC:1990:145
Sentencia	Sala 1ª	37/1989	15/02/1989	ES:TC:1989:37
Sentencia	Sala 1ª	110/1984	26/11/1984	ES:TC:1984:110

Resolución	Sala/Sección	Número	Fecha	ECLI
Sentencia	Sala 2ª	22/1984	17/02/1984	ES:TC:1984:22

II. TRIBUNAL SUPREMO

Resolución	Tribunal, Sala	Número	Fecha	ECLI
Sentencia	Sala 2ª, de lo Penal	287/2017	19/04/2017	ES:TS:2017:1487
Sentencia	Sala 2ª, de lo Penal	991/2016	12/01/2017	ES:TS:2017:47
Sentencia	Sala 2ª, de lo Penal	717/2016	27/09/2016	ES:TS:2016:4173
Sentencia	Sala 2ª, de lo Penal	656/2016	18/07/2016	ES:TS:2016:3789
Sentencia	Sala 2ª, de lo Penal	469/2016	31/05/2016	ES:TS:2016:2586
Sentencia	Sala 2ª, de lo Penal	426/2016	19/05/2016	ES:TS:2016:2149
Sentencia	Sala 2ª, de lo Penal	292/2016	07/04/2016	ES:TS:2016:1545
Sentencia	Sala 2ª, de lo Penal	284/2016	06/04/2016	ES:TS:2016:1495
Sentencia	Sala 2ª, de lo Penal	204/2016	10/03/2016	ES:TS:2016:1218
Sentencia	Sala 2ª, de lo Penal	864/2015	10/12/2015	ES:TS:2015:5809
Sentencia	Sala 2ª, de lo Penal	811/2015	09/12/2015	ES:TS:2015:5213
Sentencia	Sala 2ª, de lo Penal	786/2015	04/12/2015	ES:TS:2015:5362
Sentencia	Sala 2ª, de lo Penal	656/2015	10/11/2015	ES:TS:2015:4803
Sentencia	Sala 2ª, de lo Penal	692/2015	03/11/2015	ES:TS:2015:4809
Sentencia	Sala 2ª, de lo Penal	484/2015	07/09/2015	ES:TS:2015:3981
Sentencia	Sala 2ª, de lo Penal	187/2015	14/04/2015	ES:TS:2015:1922
Sentencia	Sala 2ª, de lo Penal	157/2015	09/03/2015	ES:TS:2015:1397
Sentencia	Sala 2ª, de lo Penal	97/2015	24/02/2015	ES:TS:2015:823
Sentencia	Sala 2ª, de lo Penal	814/2014	09/11/2014	ES:TS:2014:5068
Sentencia	Sala 2ª, de lo Penal	689/2014	21/10/2014	ES:TS:2014:4829
Sentencia	Sala 2ª, de lo Penal	513/2014	24/06/2014	ES:TS:2014:2906
Sentencia	Sala 2ª, de lo Penal	187/2014	10/03/2014	ES:TS:2014:1402
Sentencia	Sala 2ª, de lo Penal	58/2014	06/02/2014	ES:TS:2014:481
Sentencia	Sala 2ª, de lo Penal	1025/2013	26/12/2013	ES:TS:2013:6486
Auto	Sala 2ª, de lo Penal	1731/2013	26/12/2013	ES:TS:2013:8899A
Sentencia	Sala 2ª, de lo Penal	830/2013	07/11/2013	ES:TS:2013:5515

Resolución	Tribunal, Sala	Número	Fecha	ECLI
Sentencia	Sala 2ª, de lo Penal	773/2013	22/10/2013	ES:TS:2013:5060
Sentencia	Sala 2ª, de lo Penal	688/2013	30/09/2013	ES:TS:2013:4761
Sentencia	Sala 2ª, de lo Penal	1046/2013	22/07/2013	ES:TS:2013:4300
Sentencia	Sala 2ª, de lo Penal	342/2013	17/04/2013	ES:TS:2013:2222
Sentencia	Sala 2ª, de lo Penal	165/2013	26/03/2013	ES:TS:2013:1649
Auto	Sala 2ª, de lo Penal	392/2013	14/02/2013	ES:TS:2013:1800A
Sentencia	Sala 2ª, de lo Penal	987/2012	13/12/2012	ES:TS:2012:8316
Sentencia	Sala 2ª, de lo Penal	974/2012	05/12/2012	ES:TS:2012:8701
Sentencia	Sala 2ª, de lo Penal	1072/2012	11/11/2012	ES:TS:2012:9120
Sentencia	Sala 2ª, de lo Penal	740/2012	10/10/2012	ES:TS:2012:6147
Sentencia	Sala 2ª, de lo Penal	765/2012	27/09/2012	ES:TS:2012:6339
Sentencia	Sala 2ª, de lo Penal	444/2012	21/05/2012	ES:TS:2012:4189
Sentencia	Sala 2ª, de lo Penal	79/2012	09/02/2012	ES:TS:2012:414
Sentencia	Sala 2ª, de lo Penal	940/2011	27/09/2011	ES:TS:2011:5856
Sentencia	Sala 2ª, de lo Penal	861/2011	30/06/2011	ES:TS:2011:5677
Sentencia	Sala 2ª, de lo Penal	169/2011	18/03/2011	ES:TS:2011:1474
Sentencia	Sala 2ª, de lo Penal	167/2010	24/02/2010	ES:TS:2010:758
Sentencia	Sala 2ª, de lo Penal	111/2010	24/02/2010	ES:TS:2010:966
Sentencia	Sala 2ª, de lo Penal	1165/2009	24/11/2009	ES:TS:2009:7014
Sentencia	Sala 2ª, de lo Penal	932/2009	17/09/2009	ES:TS:2009:6230
Sentencia	Sala 2ª, de lo Penal	480/2009	22/05/2009	ES:TS:2009:3057
Sentencia	Sala 2ª, de lo Penal	151/2009	11/02/2009	ES:TS:2009:750
Sentencia	Sala 2ª, de lo Penal	671/2008	22/10/2008	ES:TS:2008:6245
Sentencia	Sala 2ª, de lo Penal	256/2008	14/05/2008	ES:TS:2008:2809
Sentencia	Sala 2ª, de lo Penal	894/2007	31/10/2007	ES:TS:2007:7231
Sentencia	Sala 2ª, de lo Penal	782/2007	03/10/2007	ES:TS:2007:6379
Sentencia	Sala 2ª, de lo Penal	1009/2006	18/10/2006	ES:TS:2006:6570
Sentencia	Sala 2ª, de lo Penal	151/2006	20/02/2006	ES:TS:2006:717
Sentencia	Sala 2ª, de lo Penal	1448/2005	18/11/2005	ES:TS:2005:7155
Sentencia	Sala 2ª, de lo Penal	919/2004	12/07/2004	ES:TS:2004:5000

Resolución	Tribunal, Sala	Número	Fecha	ECLI
Sentencia	Sala 2ª, de lo Penal	774/2004	16/06/2004	ES:TS:2004:4188
Sentencia	Sala 2ª, de lo Penal	384/2004	22/03/2004	ES:TS:2004:1912
Sentencia	Sala 2ª, de lo Penal	1406/2003	29/10/2003	ES:TS:2003:6699
Sentencia	Sala 2ª, de lo Penal	158/2003	05/02/2003	ES:TS:2003:705
Sentencia	Sala 2ª, de lo Penal	1803/2002	04/11/2002	ES:TS:2002:7291
Sentencia	Sala 2ª, de lo Penal	576/2002	03/09/2002	ES:TS:2002:5781
Sentencia	Sala 2ª, de lo Penal	624/2002	10/04/2002	ES:TS:2002:2529
Sentencia	Sala 2ª, de lo Penal	1335/2001	19/07/2001	ES:TS:2001:6389
Sentencia	Sala 2ª, de lo Penal	1212/2001	22/06/2001	ES:TS:2001:5386
Sentencia	Sala 2ª, de lo Penal	1066/2001	06/06/2001	ES:TS:2001:4770
Sentencia	Sala 2ª, de lo Penal	698/2001	28/04/2001	ES:TS:2001:3471
Sentencia	Sala 2ª, de lo Penal	550/2001	03/04/2001	ES:TS:2001:2769
Sentencia	Sala 2ª, de lo Penal	543/2001	16/03/2001	ES:TS:2001:2127
Sentencia	Sala 2ª, de lo Penal	84/2001	29/01/2001	ES:TS:2001:503
Sentencia	Sala 2ª, de lo Penal	831/2000	16/05/2000	ES:TS:2000:3929
Sentencia	Sala 2ª, de lo Penal	1534/1999	16/12/1999	ES:TS:1999:8093
Sentencia	Sala 2ª, de lo Penal	1599/1999	15/11/1999	ES:TS:1999:7208
Sentencia	Sala 2ª, de lo Penal	1431/1999	13/10/1999	ES:TS:1999:6351
Sentencia	Sala 2ª, de lo Penal	1669/1999	19/05/1999	ES:TS:1999:7344
Sentencia	Sala 2ª, de lo Penal	1522/1998	02/12/1998	ES:TS:1998:7234
Sentencia	Sala 2ª, de lo Penal	1185/1998	08/10/1998	ES:TS:1998:5733
Sentencia	Sala 2ª, de lo Penal	42/1998	23/01/1998	ES:TS:1998:345
Sentencia	Sala 2ª, de lo Penal	1413/1997	21/11/1997	ES:TS:1997:7012
Sentencia	Sala 2ª, de lo Penal	1140/1997	23/09/1997	ES:TS:1997:5605
Sentencia	Sala 2ª, de lo Penal	999/1997	27/06/1997	ES:TS:1997:4566
Sentencia	Sala 2ª, de lo Penal	181/1997	15/02/1997	ES:TS:1997:1041
Sentencia	Sala 2ª, de lo Penal	721/1996	18/10/1996	ES:TS:1996:5648
Sentencia	Sala 2ª, de lo Penal	538/1996	11/07/1996	ES:TS:1996:4272
Sentencia	Sala 2ª, de lo Penal	379/1996	30/04/1996	ES:TS:1996:2600
Sentencia	Sala 2ª, de lo Penal	352/1996	25/04/1996	ES:TS:1996:2495

Resolución	Tribunal, Sala	Número	Fecha	ECLI
Sentencia	Sala 2ª, de lo Penal	-	06/07/1995	ES:TS:1995:3988
Sentencia	Sala 2ª, de lo Penal	-	10/10/1994	ES:TS:1994:13875
Sentencia	Sala 2ª, de lo Penal	-	11/10/1993	ES:TS:1993:6740

III. TRIBUNAL SUPERIOR DE JUSTICIA

Sede (Sala)	Número	Fecha	ECLI
Madrid (Sala de lo Social)	531/2017	19/07/2017	ES:TSJM:2017:9285
Madrid (Sala de lo Social)	696/2004	06/07/2004	ES:TSJM:2004:9328
Andalucía (Sala de lo Social)	145/2000	28/01/2000	ES:TSJAND:2000:1430

IV. AUDIENCIA PROVINCIAL

Provincia (Sección)	Número	Fecha	ECLI
Guadalajara (Secc. 1)	8/2016	04/04/2016	ES:APGU:2016:134
Madrid (Secc. 17)	382/2015	21/05/2015	ES:APM:2015:6740
Cádiz (Secc. 3)	31/2014	28/01/2014	ES:APCA:2014:122
Pontevedra (Secc. 4)	10/2014	10/01/2014	ES:APPO:2014:18
A Coruña (Secc. 6)	268/2013	11/11/2013	ES:APC:2013:2875
Madrid (Secc. 27)	12/2013	05/04/2013	ES:APM:2013:5798

V. TRIBUNAL EUROPEO DERECHOS HUMANOS

Resolución	Fecha	Caso	ECLI
Sentencia	03/07/2012	Robathin contra Austria	CE:ECHR:2012:0703JUD003045706
Sentencia	22/05/2008	Iliya Stefanov contra Bulgaria	CE:ECHR:2008:0522JUD006575501
Sentencia	13/03/2007	Castravet contra Moldavia	CE:ECHR:2007:0313JUD002339305
Sentencia	05/10/2006	Viola contra Italia	CE:ECHR:2006:1005JUD004510604
Sentencia	26/09/2006	Abdulkadir Coban contra España	CE:ECHR:2006:0925DEC001706002
Sentencia	18/02/2003	Prado Burgallo contra España	CE:ECHR:2011:1018DEC002121809
Sentencia	20/06/2000	Foxley contra Reino Unido	CE:ECHR:2000:0620JUD003327496

Sentencia	25/06/1997	Halford contra Reino Unido	CE:ECHR:1997:0625JUD002060592
Sentencia	16/12/1992	Niemietz contra Alemania	CE:ECHR:1992:1216JUD001371088
Sentencia	30/07/1988	Valenzuela Contreras contra España	CE:ECHR:1998:0730JUD002767195